2014-09

Collective impact and its application to the domestic intelligence enterprise

Noce, Vincent E.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

COLLECTIVE IMPACT AND ITS APPLICATION TO THE DOMESTIC INTELLIGENCE ENTERPRISE

by

Vincent E. Noce

September 2014

Thesis Advisor:	Erik J. Dahl
Second Reader	John Rollins

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
COLLECTIVE IMPACT AND ITS APPLICATION TO THE DOMESTIC INTELLIGENCE ENTERPRISE

5. FUNDING NUMBERS

6. AUTHOR(S) Vincent E. Noce

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

For the past 40 years, the United States has implemented what is tantamount to a de facto domestic intelligence enterprise, which is comprised of a constellation of several state, local, and federal partners. It could be reasonably stated that these partners came into being for a few different reasons, (1) to demonstrate action following seminal event or crisis, (2) to address an unmet or previously unanticipated need, or (3) to comply with a policy or legal initiative. Since the terrorist attacks of September 11, 2001, several national strategies and information-sharing initiatives have been implemented that compel these entities to engage in more robust collaborative activities.

This thesis summarizes three selected elements of the domestic intelligence enterprise, which are missioned to provide a variety of services to state and local homeland security stakeholders, and introduces the concept of collective impact as a possible framework for enhanced collaboration. Additionally, it examines how each element, within its internal network, may already be practicing the core concepts of collective impact and offers recommendations for how cross-network implementation of collective impact may benefit each element and produce efficiencies within the domestic intelligence enterprise.

14. SUBJECT TERMS: intelligence, collaboration, collective impact, inter-agency collaborative capacity, fusion centers, high intensity drug trafficking area, investigative support center, regional information sharing system

15. NUMBER OF PAGES 97

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

COLLECTIVE IMPACT AND ITS APPLICATION TO THE DOMESTIC INTELLIGENCE ENTERPRISE

Vincent E. Noce
Staff Officer, Mississippi Office of Homeland Security,
B.A., Marquette University, 1992

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2014**

Author: Vincent E. Noce

Approved by: Erik J. Dahl
Thesis Advisor

John Rollins
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

For the past 40 years, the United States has implemented what is tantamount to a de facto domestic intelligence enterprise, which is comprised of a constellation of several state, local, and federal partners. It could be reasonably stated that these partners came into being for a few different reasons, (1) to demonstrate action following seminal event or crisis, (2) to address an unmet or previously unanticipated need, or (3) to comply with a policy or legal initiative. Since the terrorist attacks of September 11, 2001, several national strategies and information-sharing initiatives have been implemented that compel these entities to engage in more robust collaborative activities.

This thesis summarizes three selected elements of the domestic intelligence enterprise, which are missioned to provide a variety of services to state and local homeland security stakeholders, and introduces the concept of collective impact as a possible framework for enhanced collaboration. Additionally, it examines how each element, within its internal network, may already be practicing the core concepts of collective impact and offers recommendations for how cross-network implementation of collective impact may benefit each element and produce efficiencies within the domestic intelligence enterprise.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ATIX™	Automated Trusted Information Exchange
BJA	Bureau of Justice Assistance
CI	Collective Impact
COC	Critical Operating Capability
DCI	Director of Central Intelligence
DHS	Department of Homeland Security
DOJ	Department of Justice
EC	Enabling Capability
EPIC	El Paso Intelligence Center
FBI	Federal Bureau of Investigation
FCPP	Fusion Center Performance Program
FIG	Field Intelligence Group
FinCEN	Financial Crimes Enforcement Network
GAO	General Accountability Office
HIDTA	High Intensity Drug Trafficking Area
HSEC SINs	Homeland Security Standing Information Needs
HSIN	Homeland Security Information Network
I&A	Intelligence & Analysis
ICC	Inter-Agency Collaborative Capacity
IIR	Institute for Intergovernmental Research
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISC	Investigative Support Center
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
MAGLOCLEN	Middle Atlantic Great Lakes Organized Crime Law Enforcement Network
MOCIC	Mid-States Organized Crime Information Center
NCISP	National Criminal Intelligence Sharing Plan
NESPIN	New England State Police Information Network
NNFC	National Network of Fusion Centers

OCDETF	Organized Crime Drug Enforcement Task Forces
ONDCP	Office of National Drug Control Policy
P/CRCL	Privacy, Civil Rights and Civil Liberties
PINs	priority information needs
RISS	Regional Information Sharing Center
RMIN	Rocky Mountain Information Network
RNPG	RISS National Policy Group
ROCIC	Regional Organized Crime Information Network
SBU	sensitive but unclassified
SINs	standing information needs
SLPO	State and Local Program Office
U.S.	United States
WSIN	Western States Information Network

EXECUTIVE SUMMARY

Over the past 40 years, the United States has implemented a de facto domestic intelligence enterprise that is comprised of a constellation of over 268 local, state, and federal partners.[1] It could be argued that most of the elements of the enterprise came into existence by one of three means: in response to a crisis, to fulfill an unmet need, or to satisfy the requirements of legislative action. For the purpose of this thesis, the elements of the domestic intelligence enterprise examined are state and local fusion centers, high intensity drug trafficking area (HIDTA) investigative support centers (ISCs), and regional information sharing system (RISS) centers. These elements were chosen because they are comprised of networks, which are "closest to the ground." In other words, they are specifically missioned to support state and local law enforcement, and ostensibly, those closest to the greatest volume of raw information.

Whether the problem set is narcotics, terrorism, or organized crime, it could be said that each of the elements has been engaged in a pattern of Isolated Impact, which assumes the following. Funds are allocated to individual organizations that offer the most promising solutions, those organizations work separately and compete to produce the greatest independent impact, evaluation of efforts is isolated to that organization, and larger-scale progress against the problem is dependent upon scaling a single organization.[2] This begs the question, and provides the underlying inquiry of this thesis. Do independent, isolated *efforts* only represent a surrogate for real *impact* against the issue, or might a better framework exist for cross-element collaboration? Therefore, the primary question this thesis intends to ask is if a common framework for collaboration should be adopted between these elements in an effort to better

[1] Brian A. Jackson, ed. *Considering the Creation of a Domestic Intelligence Agency in the United States: Lessons learned from the Experiences of Australia, Canada, France, Germany, and the United Kingdom* (Santa Monica, CA: The Rand Corporation, 2009).

[2] John Kania and Mark Kramer, "Collective Impact," *Stanford Social Innovation Review* 1, no. 9 (2011): 36–41.

coordinate activities and evaluate the impact of their operation. This thesis introduces the collaborative framework of collective impact (CI) as it has been applied in the realm of non-profit organizations and investigates how it may apply to selected elements of the domestic intelligence enterprise. Whereas CI is defined as "the commitment of a group of actors from different sectors to a common agenda for solving a complex social problem,"[3] it assumes that the following five conditions exist within any problem space with which the three elements wish to collaborate.

- Common Agenda
- Shared Measurement
- Mutually Reinforcing Activities
- Continuous Communication
- Backbone Support[4]

One of the key findings discovered through the research process was that the three elements examined might already be leveraging key concepts associated with CI *within* their networks. However, opportunities exist for these elements to enhance the CI model of collaboration *between* the networks. Finally, strong evidence is available in the form of some new and existing regional and cross-element projects that demonstrate the desire to enhance collaboration in innovative ways. These advances, however, could be bolstered by additional work and inquiry in the following areas.

- Consideration of policy changes with respect to funding that allow for longer-term planning with respect to strategic goals
- Mutually shared collection and reporting priorities across the enterprise
- Continued federation of technology platforms

[3] Kania and Kramer, "Collective Impact," 36–41.

[4] Ibid.

- Development of common metrics and measures that empirically illustrate the relationship between information sharing and impact on a problem set

- Recognition of the value of competitive analysis by including all elements of the enterprise in exercises and “red team” operations

No doubt exists that the domestic intelligence enterprise in the United States serves a very impactful purpose and the capabilities built have enhanced and encouraged collaboration on levels never before imagined. Whether established by legal mandate, in response to a crisis, or a natural need to cooperate, deliberate and planned collaboration has replaced most of the “random acts of partnership”[5] from the past. However, giving credit to the successes to date, any enterprise, which is so complex and has such a far-reaching mission, can benefit from the innovation and fresh inquiry collective impact offers.

[5] “The ‘How To’ Guide,’ Collaboration for Impact,” accessed July 15, 2014, http://www.collaborationforimpact.com/the-how-to-guide/.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would first like to dedicate this effort to my parents, who always impressed upon me the importance of education and the truth that learning is a lifelong process. I would also like to thank my sisters and my friends who have endured this process with me and supported me with their understanding and encouragement.

To the amazing instructors and staff at the Center for Homeland Defense and Security, your time, support and expertise made this entire process possible. I would also like to thank the members of Cohorts 1301 and 1302. The collaboration and fellowship we shared both inside the classroom and out made the entire course enjoyable. I am truly honored to count you among my colleagues.

Finally, to my advisor and second reader, Erik Dahl and John Rollins. Without your patience and leadership, this effort would not have come to completion. In addition, to Dr. Bellavita, whose article presented a new framework of thought for me, thank you for your inspiration.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In tackling information issues, America needs unity of effort.

–The 9/11 Commission Report

Soon after the terrorist attacks of September 11, 2001, policy makers in the United States (U.S.) began to debate and examine ways to improve how the country does the business of intelligence, information sharing, and domestic security. One of the most profound actions the U.S. government took following the terrorist attacks resulted in the largest reorganization of government in the republic's history. The newly-created U.S. Department of Homeland Security (DHS) combined, amalgamated, and merged all or part of 22 different departments into a single cabinet-level organization in an effort to form a single, unified homeland security structure tasked to "improve protection against today's threats and be flexible enough to help meet the unknown threats of the future.[1] In addition, in a further effort to remedy the well-documented intelligence and information-sharing failures leading up to September 11, 2001, President George W. Bush proposed that:

> [T]he new Department would contain a unit whose sole mission is to assemble, fuse, and analyze relevant intelligence data from government sources, including CIA, NSA, FBI, INS, DEA, DOE, Customs, and DOT, and data gleaned from other organizations and public sources. With this big-picture view, the Department would be more likely to spot trends and would be able to direct resources at a moment's notice to help thwart a terrorist attack.[2]

[1] George W. Bush, *The Department of Homeland Security* (Washington, DC: Department of Homeland Security, June 2002).

[2] Ibid.

Additionally, claiming, "the Federal Bureau of Investigation had failed to merge properly and perform effectively its dual missions of law enforcement and the collection, analysis, and dissemination of foreign intelligence inside the United States,"[3] Senator Edwards introduced a bill in 2003 titled the *Foreign Intelligence Collection Improvement Act of 2003*. The bill advocated for the establishment of a new member of the United States Intelligence Community called the Homeland Intelligence Agency.[4] Although unsuccessful, Edwards' bill recognized the importance of the state and local role in the larger intelligence community.

While each of the efforts mentioned above shows the importance of, and strategic intent to identify, formalize, and in some cases, create new relationships between existing intelligence practitioners, the United States chose not to pursue the creation of a single domestic intelligence agency. Rather, it chose the path of reform through creating an environment of greater collaboration and engagement with state and local entities, and with existing organizations, which were already engaged in the collection and analysis of criminal intelligence.

The goal of this thesis is to introduce a new framework of collaboration for similar elements of the domestic intelligence enterprise, and make recommendations, which may increase the effectiveness and impact of those entities. The next section of this chapter provides an overview of the domestic intelligence enterprise at large, and the following section describes the importance of collaboration and introduces the concept of collective impact (CI).

---

[3] *Foreign Intelligence Collection Improvement Act of 2003*.

[4] Todd Masse, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States* (CRS Report No. RL31920) (Washington, DC: Congressional Research Service, 2003).

A. OVERVIEW OF THE AMERICAN DOMESTIC INTELLIGENCE ENTERPRISE

Over the past 40 years, the United States has implemented several elements of what could be construed to be a domestic intelligence enterprise (enterprise), with the most recent addition being the national network of fusion centers. It could be accurately stated that each of the elements of the enterprise came into being as a response to three different, albeit abstractly related reasons: (1) to demonstrate action following a seminal event or crisis, (2) to address an unmet or previously unanticipated need, or (3) to comply with a policy or legal initiative. In its current state, the enterprise in the United States is comprised of a constellation of state, local, and federal partners, and while no consensus definition of domestic intelligence has been established in law or public policy,[5] the Rand Corporation defines it as:

> Efforts by government organizations to gather, assess and act on information about individuals or organizations in the United States or U.S. persons elsewhere that is not necessarily related to the investigation of a known past criminal act or specific planned criminal activity.[6]

In President George W. Bush's *2002* National *Homeland Security Strategy*, the DHS, the Director of Central Intelligence (DCI) and Federal Bureau of Investigation (FBI) were identified as the primary responsible parties for information and analysis relating to homeland security (as indicated in Figure 1).

---

[5] Todd Masse, Siobhan O'Neil, and John Rollins, *Fusion Centers: Issues and Options for Congress* (CRS Report No. RL34070) (Washington, DC: Congressional Research Service, 2007).

[6] Gregory F. Treverton, "Reorganizing U.S. Domestic Intelligence, Assessing the Options," RAND Corporation, accessed November 16, 2013, http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG767.pdf.

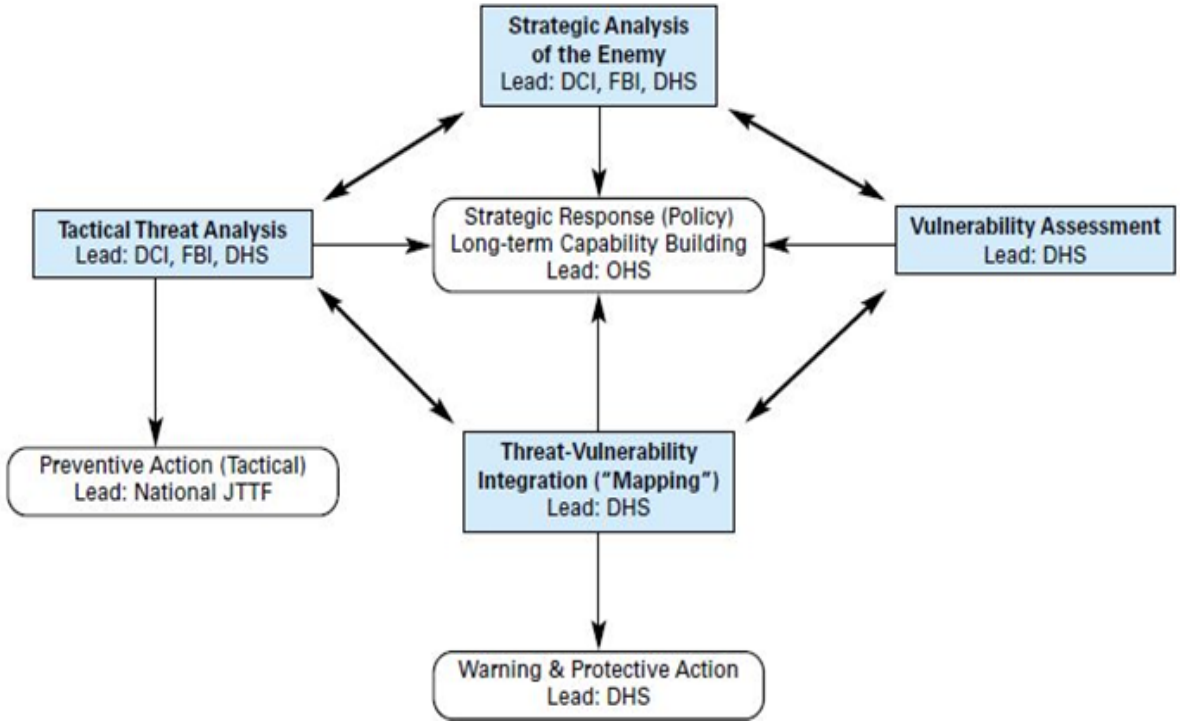

Figure 1. Roles and Responsibilities of Homeland Security Intelligence and Information Analysis[7]

In addition to the groups in Figure 1, other principal entities currently comprising the enterprise are the following.

- **FBI Field Intelligence Groups (FIG)**—Part of the FBI, this group supports FBI investigations through the collection and analysis of intelligence, and creates a variety of analytical products to inform the FBI's law enforcement and intelligence partners.

- **Regional Information Sharing System (RISS) Centers**—Funded by the Department of Justice (DOJ), this component supports regional law enforcement, public safety, and homeland security efforts to combat major crime and terrorist activity.

[7] George W. Bush, *The Department of Homeland Security* (Washington, DC: Department of Homeland Security, June 2002).

- **State and Major Urban Area Fusion Centers**—Funded through a variety of federal and state resources, and in part through DHS and DOJ grants, fusion centers are state and locally owned, and operate as intermediaries for sharing terrorism and other threat-related information between the federal government and state, local, tribal, territorial, and private-sector homeland security partners.

- **High Intensity Drug Trafficking Areas (HIDTA) Investigative Support Centers (ISC)**—Funded through grants administered by the Office of National Drug Control Policy (ONDCP), HIDTA ISCs aim to support the disruption and dismantlement of drug-trafficking and money-laundering organizations through the prevention and mitigation of associated activity.[8]

Further, as of January 2013, 268 units of five major types of field-based entities (FBI joint terrorism task force, FBI field intelligence Group, regional information sharing centers, state and local fusion centers, and high intensity drug trafficking area investigative support centers), many co-located with one another, were situated throughout the United States (as illustrated in Figure 2).[9]

[8] Government Accountability Office, *Information Sharing. Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities* (GAO-13-471) (Washington, DC: U.S. Government Accountability Office, 2013), 1–2.

[9] Ibid.

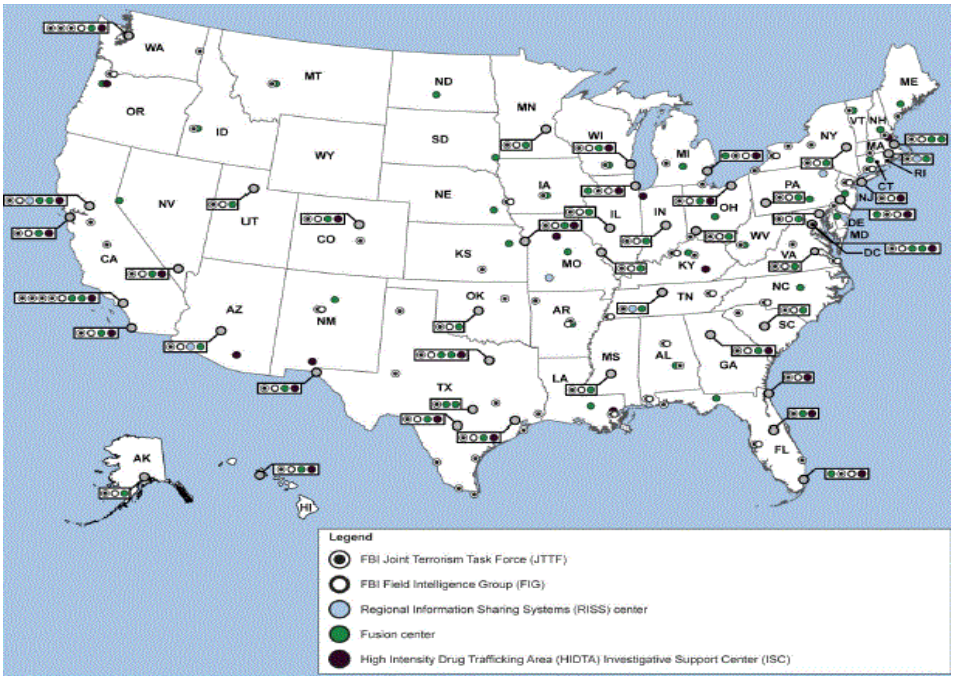

Figure 2. Geographic Location of Selected Elements of the Domestic Intelligence Enterprise[10]

Figure 3 more visually represents the network structure of the enterprise and illustrates: (1) how loosely, if at all, each of the elements is connected, (2) how each is organized around a specific mission set, and (3) how these partners could become isolated from one another and the larger network without strong collaborative ties.

[10] Government Accountability Office, *Information Sharing. Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities*, 1–2.

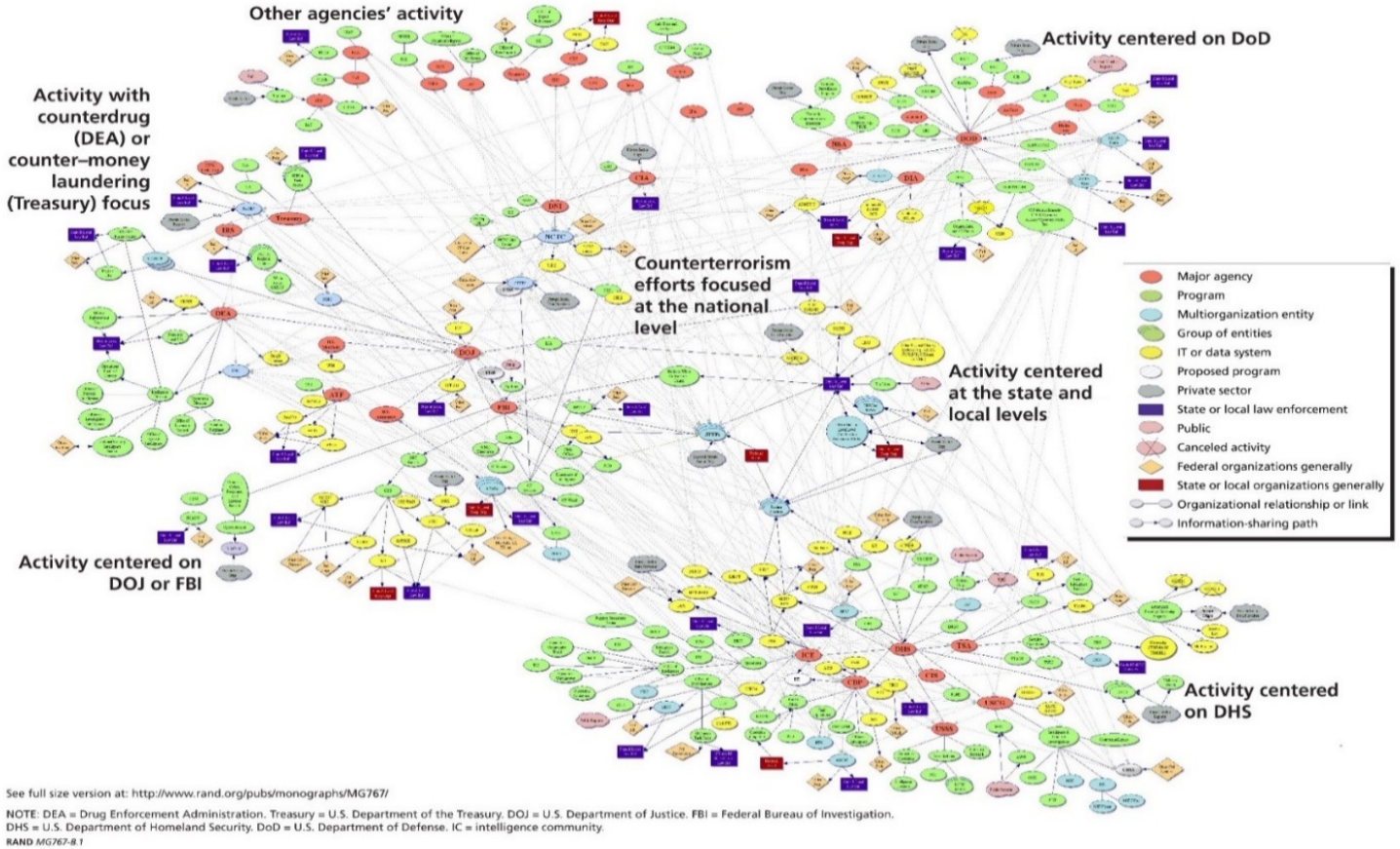

Figure 3. Network Structure of the Enterprise[1]

[1] Treverton, "Reorganizing U.S. Domestic Intelligence, Assessing the Options," 112. The image can also be found at http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG767.figureB1.pdf.

B. WHY COLLABORATION IS IMPORTANT IN THE PRACTICE OF HOMELAND SECURITY

One of the underlying and perhaps most critical missions of the DHS is improving the effectiveness of collaboration and information sharing among all levels of government within the United States. This nation's weakness in these areas was exploited by al-Qaeda in the lead up to the terrorist attacks of September 11, 2001. In addition, considering the findings of the *9/11 Commission Report*, collaboration, or joint action, stands to benefit all involved in the homeland security practice by engaging in joint planning, ensuring a unified effort by identifying definitive leadership, and mitigating the gaps created by critical shortages of experts.[1] While it will never be possible to know if these activities would have prevented the attacks, it stands to reason that a culture of "need to share" rather than "need to know"[2] prior to September 11, 2001 could have increased the odds of seizing on any one of the 10 operational opportunities to disrupt the attacks identified by the 9/11 Commission.[3]

While not related to terrorism, but nonetheless important, the response to Hurricane Katrina again exposed U.S. vulnerabilities within and across organizational and jurisdictional boundaries. Throughout the event, a number of breakdowns in collaboration were evident: a lack of information sharing among agencies, confused inter-organizational relationships, competing roles and responsibilities, and shortcomings in leadership.[4]

The response to man-made and natural disasters have many things in common, the most impactful of which may be that they are both complex

---

[1] Thomas H. Kean and Lee Hamilton, *National Commission on Terrorist Attacks upon the United States, The 9/11 Commission report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004), 401.

[2] Ibid., 24.

[3] Ibid., 8–9.

[4] Susan Page Hocevar, Gail Fann Thomas, and Erik Jansen, "Inter-Organizational Collaboration: Addressing the Challenge," *Homeland Security Affairs* 7, The 9/11 Essays (September 2011): 4.

problems that require capabilities of many disciplines that have both aligned and competing interests, and usually function without an over-arching command authority.[5] With the recent designation of the intelligence/investigations function as a section level stakeholder in the National Incident Management System,[6] and with a substantial number of state and local fusion centers co-located with either state or local emergency operations centers,[7] and supporting all-hazards missions, the collection, analysis, and dissemination of threat information by fusion centers can inform both preplanning response activities, as well as operational response and coordination efforts during and after an incident or event.[8]

C. RESEARCH QUESTION

Within key elements of the domestic intelligence enterprise—state and local fusion centers, RISS, and ISC—a shared mission exists, and in some cases, the entities are co-located. Considering these similarities, should the state and local fusion centers, RISS Centers and HIDTA ISCs adopt a common framework for collaboration and evaluation to coordinate activities and evaluate the impact of their operations better? Since the elements of the enterprise selected for this thesis are very similar, this thesis argues that the concept of CI offers such a common framework.

D. LITERATURE REVIEW

As the concept of CI is a newer approach to collaboration, limited scholarly research is available for study. However, several case studies and

---

[5] Ibid.

[6] Department of Homeland Security, *NIMS Intelligence/Investigations Function Field Operations Guide* (Washington, DC: Department of Homeland Security, 2013).

[7] Seventy-one percent of state and local fusion centers have an all-hazards mission; 46% are co-located with a state or local emergency operations center; and 58% assign personnel to emergency management and/or emergency operations centers during events or incidents.

[8] Department of Homeland Security, *Fusion Center and Emergency Management Collaboration Meeting After-Action Report* (Washington, DC: Department of Homeland Security, 2014).

historical examples of what can be categorized as CI before the idea was labeled as such do exist. In general, CI is a new way of framing collaborative efforts around a common goal. The area in which CI may differ from other collaborative frameworks is the stipulation that each group wishing to participate in the collaborative effort must relinquish, to some degree, its individual agenda in the pursuit of the overall objective. This literature review defines and describes the domestic intelligence enterprise in the United States, and also summarizes other writing on collaboration.

1. The Domestic Intelligence Enterprise, in General

> Homeland security is a uniquely American concept. It is a product of American geographic isolation and the strong tendency throughout American history to believe that there was a clear divide between events, issues and problems outside the U.S. borders and those inside the U.S. Borders.[9]

However, many countries around the world have been engaged in practices similar to the American concept for many years whose efforts may be instructive, albeit without the considerable constraints and protections of the U.S. Constitution.[10] Along with the idea of a government enterprise focused on domestic security (the DHS), it could reasonably be assumed that an accompanying intelligence capability is critical to its success. Rather than establishing a monolithic national domestic intelligence structure, policy makers recognized the importance of local law enforcement as a critical component of this nation's security capability, as both "first preventers" and "first responders."[11] As a viable alternative to a national intelligence agency, experts have said that this approach is effective in that the public generally trusts local law enforcement, and it is easier to calibrate and focus. However, oversight becomes more

[9] Nadav Morag, "Does Homeland Security Exist Outside the United States?" *Homeland Security Affairs*, 7, The 9/11 Essays (September 2011): 1.

[10] Ibid.

[11] The White House, *National Strategy for Information Sharing, Success and Challenges in Improving Terrorism-Related Information Sharing* (Washington, DC: The White House, 2007), 10.

complicated with more local parties involved.[12] This shift in national security responsibility has been quietly unfolding since the attacks on September 11, 2001, as evidenced by the introduction of state and locally owned fusion centers. Despite its decentralized structure, the structure currently in place in the United States is more coordinated and also more effective than most Americans realize, and constitutes a de facto—but little understood—domestic intelligence system.[13]

2. Collaboration Matters

Collaboration and information sharing are often at the center of the intelligence debate. However, one view is consistent; intelligence and information-sharing failures, such as those that preceded the attacks of September 11, 2001, often stimulate debate to remedy what are real or perceived functional, procedural, regulatory, systemic, and/or structural problems.[14] Following the mandates of Executive Order 13356 and Section 1016 of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), an information sharing environment (ISE) was established for counterterrorism, weapons of mass destruction, and homeland security information.[15] The IRTPA also established an information-sharing council whose duties, among others, was to ensure coordination among federal partners and make recommendations as to how the ISE could be extended to incorporate appropriate state and local authorities.[16] Also, rather than mandating a centralized terrorism information database, the IRTPA required that the ISE connect existing systems, be decentralized, and allow operations among and between all levels of government as appropriate, which spurred an unprecedented level of collaboration between a

[12] "Intelligence Reform: Challenging the Conventional Wisdom Part 2," Mike German and Erik Dahl, July 15, 2014, NPS Video.

[13] Erik J. Dahl, "Domestic Intelligence Today More Security but Less Liberty?" *Homeland Security Affairs*, 7, The 9/11 Essays (September 2011): 3.

[14] Masse, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States*.

[15] 6 USC 485 Section 1016 IRTPA 1016 (b) (1) (A).

[16] Ibid., (g) (1).

vast array of stakeholders in the newly formed practice of homeland security. While not applied specifically to domestic intelligence, or the partners, which are the focus of this thesis, the General Accountability Office (GAO) conducted a study, which could be instructive to the cross-agency initiatives of the enterprise. Its 2005 study, titled *Results-Oriented Government, Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, identifies several characteristics—including leadership, trust, and organizational culture—that are necessary for a collaborative working relationship.[17]

One collaborative framework, the inter-organizational collaborative capacity (ICC) model, is defined as "the capability of organizations (or a set of organizations) to enter into, develop, and sustain inter-organizational systems in pursuit of collective outcomes."[18] What is assumed is that each of the organizations will embrace five key factors to build collaborative capacity: (1) purpose and strategy, (2) lateral processes, (3) incentives and rewards, (4) structure, and (5) people. Of particular application to the enterprise, the ICC model places several organizations in a problem space and assumes deliberate leadership and alignment of organizational design elements toward collaboration.[19]

Differing from the ICC, CI is a newer model for collaboration that is being leveraged by groups of government, nonprofit organizations, and community stakeholders. Recognizing that some tasks are larger and more complex than any one organization can effectively manage, the collective resources and talents of interested parties are pooled and focused toward a shared vision for change. Dispensing with the inefficiencies of isolated impact, in which numerous

---

[17] Government Accountability Office, *Report to the Chairman, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate. Results-Oriented Government Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies* (GAO-06-15) (Washington, DC: U.S. Government Accountability Office, October 2005).

[18] As quoted in Hocevar, Fann Thomas, and Jansen, "Inter-Organizational Collaboration: Addressing the Challenge."

[19] Ibid.

organizations separately compete for resources,[20] participants in a CI initiative agree to work cooperatively under the following five key conditions.

- Common agenda
- Shared measurement
- Mutually reinforcing activities
- Continuous communication
- Backbone support[21]

CI also assumes that the goal is long-term in nature, requires supporting infrastructure to build processes, and requires funders to shift their perspective to support a new approach.[22] While the intentions, goals and/or outputs may be similar between the two models, CI is distinctly different in that it involves a centralized infrastructure, dedicated staff, and a structured process that leads to a common agenda, shared measurement, continuous communication, and mutually reinforcing activities.[23]

In applying these theories of collaboration, CI more closely resembles a federation of organizations. In other words, the constituent elements of a federation, by definition, relinquish some degree of authority to a more central body. Moreover, the ICC more closely resembles a community, wherein it is implied that a group of persons or entities merely have common interests, but are not necessarily bound together by any formal power sharing arrangements or

[20] Fay Hanleybrown, John Kania, and Mark Kramer, "Channeling Change: Making Collective Impact Work," *Stanford Social Innovation Review*, January 26, 2012, http://www.ssireview.org/blog/entry/channeling_change_making_collective_impact_work.

[21] John Kania and Mark Kramer, "Collective Impact," *Stanford Social Innovation Review* 1, no. 9 (2011): 36–41.

[22] Chris Thompson, "Rereading Collective Impact: Three Lessons," *Stanford Social Innovation Review*, February 3, 2014.

[23] Kania and Kramer, "Collective Impact," 36–41.

agreements.[24] Considering the relatively early establishment of the RISS centers and the later addition of the HIDTA ISCs, it could be argued that state and local intelligence capabilities have been the silent backbone of larger domestic intelligence efforts for at least the past 40 years, even if only recently, they have been included in national-level strategies.

In subsequent chapters, this thesis evaluates the advantages and disadvantages of fusion centers, RISS centers and HIDTA ISCs adopting a new framework of collaboration based on CI. Chapter II introduces and further defines the concept of CI. Chapters III, IV, and V provide a brief history of each of the elements, and how they may already be using the framework. Chapter VI describes what steps could be taken to bolster the collaborative bonds of these three very similar, yet uniquely missioned organizations utilizing the CI framework, and also identifies areas of further study as they relate to the application of CI to the domestic intelligence enterprise.

[24] Mark A. Randol, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress* (CRS Report No. R40602) (Washington, DC: Congressional Research Service, 2010), 16–17.

II. ON COLLABORATION

'Tis profitable for us both, that I should labour with you today,
and that you should aid me tomorrow.

–David Hume

Although it may seem obvious that organizations accomplish more when they work together, no commonly accepted definition of collaboration exists. For the purposes of this thesis, collaboration is defined as "any joint activity by two or more organizations that is intended to produce more public value than could be produced when the organizations act alone."[25] While this definition seems simple enough, organizations can benefit from deploying a collaborative framework that more specifically defines goals, roles, responsibilities, and expected outcomes. In its 2005 study titled, *Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, the GAO identified eight practices that can enhance and sustain collaborative efforts between organizations.

- Define and articulate a common outcome
- Establish mutually reinforcing or joint strategies
- Identify and address needs by leveraging resources
- Agree on roles and responsibilities
- Establish compatible policies, procedures, and other means to operate across agency boundaries
- Develop mechanisms to monitor, evaluate, and report on results
- Reinforce agency accountability for collaborative efforts through agency plans and reports

[25] Eugene Bardach, *Getting Agencies to Work Together: The Practice and Theory of Managerial Craftsmanship* (Washington, DC: Brookings Institution, 1998).

- Reinforce individual accountability for collaborative efforts through performance management systems[26]

While the GAO's criteria are useful, it could be constructive for public managers first to consider a few more broad topics related to their prospective participation in a collaborative effort. The "strategic triangle" depicted in Figure 4 asks government managers to focus on the larger, albeit no less complex, issues that they should consider before committing themselves and their organizations to a particular course of action.

- What is the important public value the organization seeks to produce?
- What sources of legitimacy and support would be relied upon to authorize the organization to take action and provide the resources necessary to sustain the effort to create that value?
- What operational capabilities (including new investments and innovations) would the organization rely on (or have to develop) to deliver the desired results?[27]

[26] U.S. Government Accounting Office*, Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration Amount Federal Agencies* (GAO-06-15) (Washington, DC: U.S. Government Accountability Office, 2005), http://www.gao.gov/new.items/d0615.pdf.

[27] Mark Moore and Sanjeev Khagra, *On Creating Public Value: What Business Might Learn from Government about Strategic Management, Corporate Social Responsibility Initiative Working Paper No. 3* (Cambridge, MA: John F. Kennedy School of Government, Harvard University, 2004).

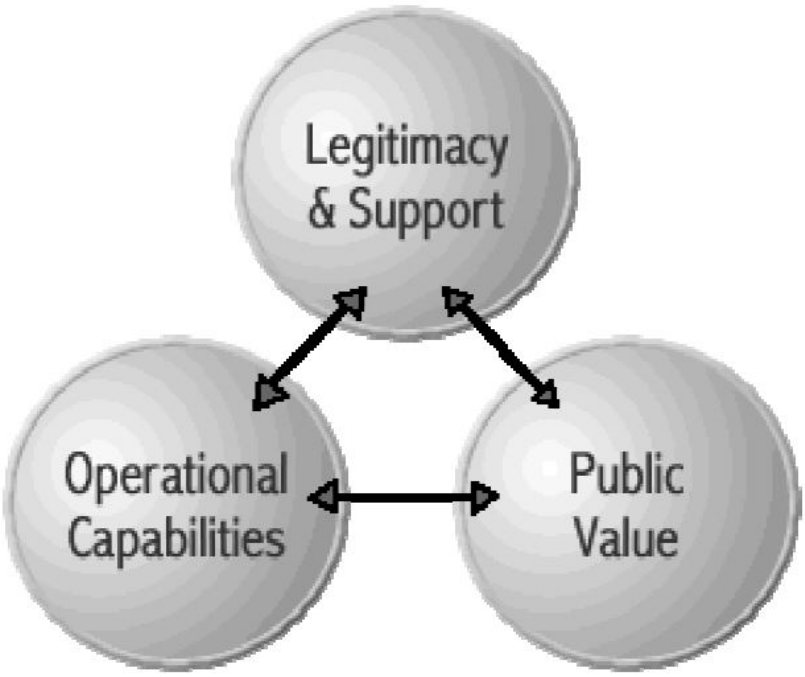

Figure 4. The Strategic Triangle[28]

Considering the above defined, and larger ideas relating to collaboration, the remainder of this chapter provides more detail with respect to two models currently being leveraged in the government and in philanthropic/non-government organization domains, ICC and CI.

A. THE ICC MODEL

While many models exist that describe collaboration, perhaps the most applicable to the domestic intelligence enterprise is the ICC model, which is illustrated in Figure 5.

[28] Moore and Khagra, *On Creating Public Value*.

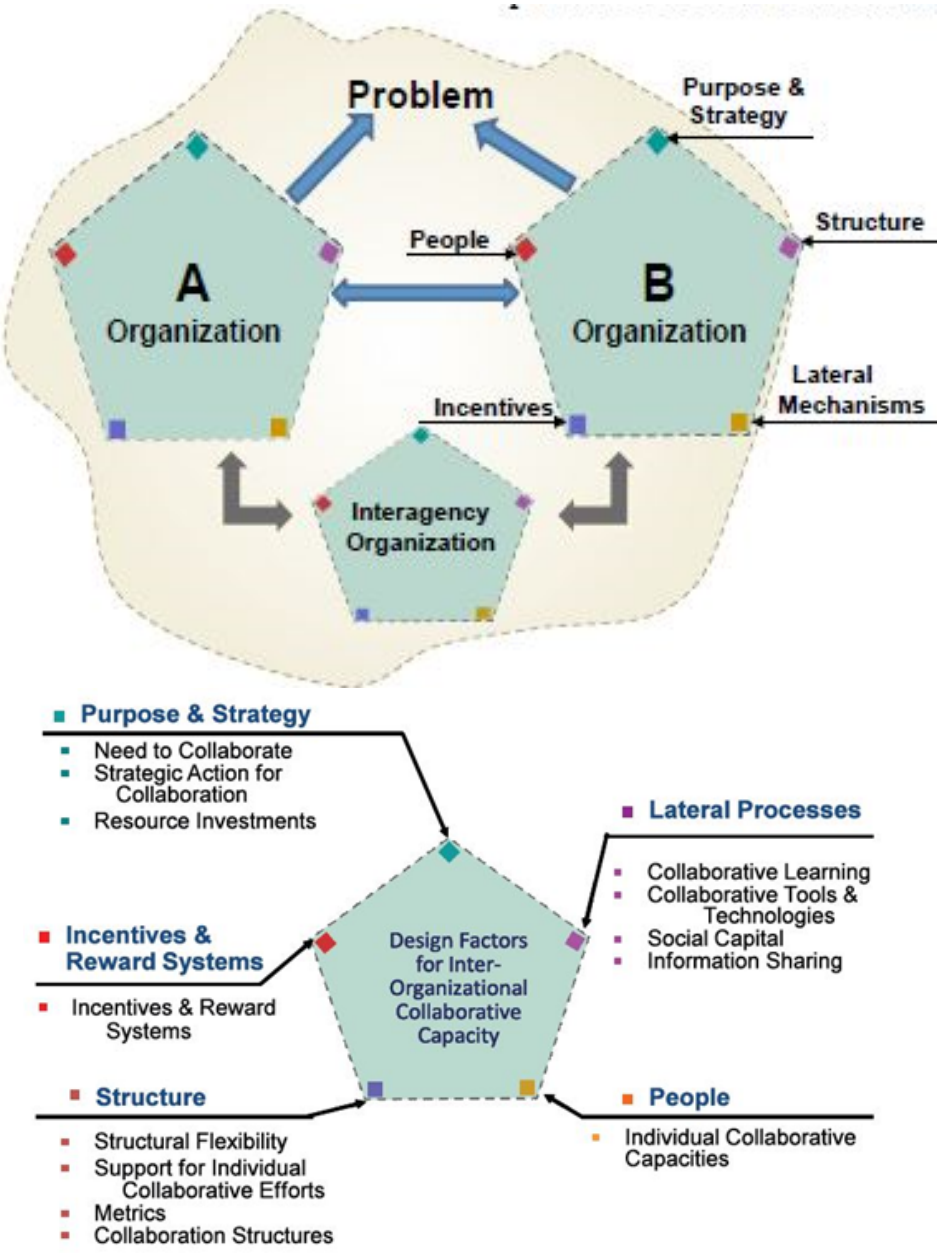

Figure 5. Organizations in a Common Problem Space[29]

The ICC model provides a mechanism to assess different factors that contribute to an organization's capacity to collaborate with other organizations. It can serve as a framework to diagnose current collaborative capabilities and provide data to guide organizational changes to improve those capabilities. The

[29] Moore and Khagra, *On Creating Public Value*.

model is comprised of five organizational domains each with their individual factors.

- *Purpose and Strategy*: It could be reasonably stated that purpose and strategy underlie any effort in which organizations desire to collaborate, and is comprised of three basic elements: (1) the need to collaborate, or *felt need*, (2) strategic action for collaboration, and (3) resource investments. *Felt need,* which is usually the catalyst for any collaborative effort, is the organization's recognition of interdependence with others and the acknowledged need to collaborate to accomplish its mission and goals effectively. This need can either arise from a perceived threat or problem, or may simply be motivated by the desire for pro-action or prevention. Strategic action considers the larger goals for the interaction and resource investments simply identify the human and monetary resources necessary to support the effort.
- *Structure:* Building on purpose and strategy; structure is necessary to define roles and responsibilities and considers flexibility when needed. Within the structure between organizations also exists opportunities for individual collaborative efforts by "boundary spanners;" it follows that the stronger the ties between these individuals, the more productive the effort. Finally, metrics identify established criteria and performance standards by which the success of the effort is evaluated.
- *Rewards and Incentives:* Impacting more the individual than the organization, rewards and incentives can include promotions and special recognition; however, individuals may also gain a sense of reward from enhanced relationships and greater job satisfaction.
- *People:* Each individual's collaborative capacity. In other words, their attitudes, skills, and knowledge have the propensity to affect the collaborative effort between organizations. In addition, an individual's conflict management skills, willingness to share decision-making responsibilities, and familiarity of how the other organizations function can impact the overall effort.
- *Lateral Mechanisms*: This domain includes the "hard" and "soft" aspects of lateral coordination. Whereas social capital and trust represent the soft aspects, collaborative tools and technology comprise the hard aspects. The two, however, are interdependent and can have a profound impact on the success, or failure of a collaborative effort.[30]

[30] Hocevar, Fann Thomas, and Jansen, "Inter-Organizational Collaboration: Addressing the Challenge."

The ICC represents more of a description of the "how" of collaboration.[31] It builds on and further develops the broad ideas of the 2005 GAO study titled *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies,* and begins to define how organizations inhabit a problem space separately, reasons why they (should) interact, and how they can build capacity together without any amalgamation.

1. Examples of Inter-Organizational Collaborative Capacity

It can reasonably argued that most state, local, and federal law enforcement task forces emulate the factors, which comprise the ICC. One example, which is especially germane to this thesis, is the FBI's Joint Terrorism Task Forces (JTTF). However, before the first JTTF was established, and ostensibly became the model for several similar such task forces; the New York City Police Department in 1979 combined federal and local law enforcement capabilities to investigate an overwhelming number of bank robberies.[32] Growing from the original successful collaboration relating to bank robberies, the first JTTF was established in New York City in 1980. Since then, the number of individuals assigned to JTTFs has grown to over 4,200 members from over 600 state and local agencies and 50 federal agencies. JTTFs have been formed in 103 cities across the United States, with a total of 71 established since the terrorist attacks of September 11.[33]

When considering the elements of ICC, it is apparent that the JTTF template, whether intentional or not, bears close resemblance as follows.

- A felt need supplements the capabilities of the FBI with the unique investigative abilities of state and local law enforcement

---

[31] U.S. Government Accounting Office*, Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration Amount Federal Agencies*.

[32] "History of the JTTF," Anti-Defamation League, The Joint Terrorism Task Force, 2005, http://archive.adl.org/learn/jttf/history_jttf.html.

[33] "Protecting America from Terrorist Attack, Our Joint Terrorism Task Forces," Federal Bureau of Investigation, accessed July 2, 2014, http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs.

- A structure is in place by way of memoranda of understanding and internal task force chain of command

- Being chosen to participate as a task force officer is often considered prestigious not only for the individual, but shows that the officers' home agency has cultivated considerable investigative talent within its ranks

- Task force officers are largely chosen because they possess a skill set desired by the FBI, chiefly among them, the ability to work effectively with a team

- Both organizations benefit from the lateral processes of one another, which presumably results in a greater impact on the issue

This model is duplicated throughout the federal government with many similar such task forces, for example: the U.S. Marshal Service's fugitive task forces, the DOJ's Organized crime drug enforcement task forces, the Internal Revenue Service's financial crimes task forces, and the U.S. Secret Service's electronic crimes task forces, and so on.

B. COLLECTIVE IMPACT

As defined in the *Stanford Social Innovation Review*, CI is "the commitment of a group of actors from different sectors to a common agenda for solving a complex social problem."[34] CI can be further described as an emerging strategy to raise awareness and advocate for social change to build consensus and momentum among diverse groups behind a common cause. Non-government organizations, non-profit organizations, and other special interest groups, sometimes in partnership with the government, are currently leveraging this strategy. While more commonly applied as an approach to secure funding, a core assumption of the CI strategy assumes that the chosen problem or issue is too large and complex for any singular group to solve, and only through coalitions of diverse cross-sector partners can an impact be made.

[34] Kania and Kramer, "Collective Impact," 36–41.

The concept and strategy of CI assumes that the five conditions in Table 1 exist and are agreed upon by each of the parties wishing to participate in the identified initiative or goal.

Table 1. Conditions of Collective Impact[35]

The Five Conditions of Collective Impact	
Common Agenda	All participants have a shared vision for change including a common understanding of the problem and a joint approach to solving it through agreed upon actions
Shared Measurement	Collecting data and measuring results consistently across all participants ensures efforts remain aligned and participants hold each other accountable.
Mutually Reinforcing Activities	Participant activities must be differentiated while still being coordinated through a mutually reinforcing plan of action.
Continuous Communication	Consistent and open communication is needed across the many players to build trust, assure mutual objectives, and create common motivation.
Backbone Support	Creating and managing collective impact requires a separate organization(s) with staff and a specific set of skills to serve as the backbone for the entire initiative and coordinate participating organizations and agencies.

As indicated in Table 2, which contrasts the features of isolated impact with those of CI, perhaps the most striking difference is that large-scale change is reliant upon the success of a single organization that would ostensibly be scaled larger to affect greater impact.[36] In contrast, CI recognizes that complex issues require collaboration and effort among several organizations with accompanying increases in cross-sector alignment and institutional learning.

[35] Kania and Kramer, “Collective Impact,” 36–41.

[36] Ibid

Table 2. Isolated Impact vs. Collective Impact[37]

Isolated Impact vs. Collective Impact	
Isolated Impact	**Collective Impact**
• Funders select individual grantees that offer the most promising solutions.	• Funders and implementers understand that social problems, and their solutions, arise from the interactions of many organizations within a larger system.
• Nonprofits work separately and compete to produce the greatest independent impact.	• Progress depends on working toward the same goal and measuring the same things.
• Evaluation attempts to isolate a particular organization's impact.	• Large-scale impact depends on increasing cross-sector alignment and learning among many organizations.
• Large-scale change is assumed to depend on scaling a single organization.	• Organizations actively coordinate their action and share lessons learned.

2. Examples of Collective Impact

a. Strive Case Study

One of the most significant examples of the successful use of the CI concept involves efforts by non-governmental organizations to improve the rate of high school graduation in the United States. Following World War II, the United States had the highest high school graduation rate in the world. Currently, this country ranks 18th out of the top 24 industrialized nations. In addition, despite billions of dollars of contributions to individual nonprofits alongside the tireless efforts of educators and administrators, system-wide progress in improving high school graduation rates has been virtually unattainable. In fact, major funders of community and social initiatives, such as education reform, teen pregnancy reduction, and increased access to medical care, etc., such as the Annenberg

[37] Kania and Kramer, "Collective Impact," 36–41.

Foundation, Ford Foundation, and Pew Charitable Trusts, have abandoned their efforts in frustration and acknowledged their lack of progress.[38]

In 2006, a nonprofit subsidiary of KnowledgeWorks[39] brought together local leaders from the greater Cincinnati and Northern Kentucky to address the student achievement crisis and improve education in the area. In the four years after the partnership was launched, Strive partners[40] improved student success in dozens of key areas across three large public school districts, and 34 of the 53 success indicators that Strive tracks have shown positive trends, including high school graduation, fourth grade reading and math scores, and the number of preschool children prepared for kindergarten.[41] Also, in its 2012–2013 *Partnership Report*, Strive partners noted that 89 percent of the partnership's measures are showing positive trends; up from 81 in the previous year, and 68 percent from the three years prior.[42]

How Did They Do It? A core group of community leaders, from classroom teachers to university presidents, decided to abandon their individual agendas in favor of a collective approach to improving student achievement. With 300 leaders agreeing to participate, the group realized that focusing on one component of the educational system would not make much of a difference unless all parts of the continuum were improved at the same time. The group also soon realized that no single organization could accomplish this improvement alone. Therefore, they first focused the entire education community upon a singular set of goals; all measured in the same way.[43] Further, the group aligned

---

[38] Ibid.

[39] KnowledgeWorks is a social enterprise focused on creating sustainable improvement in student readiness for college and careers found at http://knowledgeworks.org/.

[40] Strive Partners is a group of leaders from various sectors, including early childhood educators, school district superintendents, college and university presidents, business and non-profit leaders, and community and corporate funders who came together in 2006 to improve academic success in Greater Cincinnati's urban core.

[41] Kania and Kramer, "Collective Impact," 36–41.

[42] Strive Partnership, *Strive Partnership Report 2012–2013* (Cincinnati, OH: Strive Partnership, 2013), 5.

[43] Kania and Kramer, "Collective Impact," 36–41.

16 local funders with nine selected grantees spanning the "cradle to career" continuum.[44]

b. The Elizabeth River Project

While the term "collective impact" may be new, the concept is not. In 1993, Norfolk, Virginia's Mayor, Marjorie Mayfield Jackson, helped found the Elizabeth River Project with the mission of cleaning up the Elizabeth River in southeastern Virginia. Over 100 stakeholders, including the city governments of Chesapeake, Norfolk, Portsmouth, and Virginia Beach, joined with community groups, as well as state and federal partners including the U.S. Environmental Protection Agency and the U.S. Navy to develop an 18-point plan to restore the watershed. Fifteen years later, more than 1,000 acres of watershed land have been conserved or restored and pollution is down by more than 215 million pounds, the most severe concentrations of carcinogens have been reduced sixfold, 27 species of fish and oysters are thriving in the restored wetlands, and bald eagles have returned to nest on the shores.[45]

c. Corporate America Is Also Exploring Collective Impact

Mars America, the manufacturer of chocolate brands M&M's and Snickers, is working with non-government organizations, local governments, and direct competitors to improve the lives of over 500,000 impoverished cocoa farmers in Côte d'Ivoire, where Mars sources a large portion of its raw materials. Based on research, better farming practices and improved plant stocks could triple yields and dramatically increase the incomes of the cocoa farmers while improving the practice of Mars' supply chain.[46]

---

[44] "Quality Continuous Improvement," Strive Partnership, July 15, 2014, http://www.strivepartnership.org/priority-area-highlights.

[45] Kania and Kramer, "Collective Impact," 36–41.

[46] Ibid.

3. Potential Problems with Collective Impact

While no scholarly literature is available that challenges the viability of CI, a few arguments have been made about its potential weaknesses. Moreover, even though it may be counterintuitive to think the concept of assembling a group of organizations that share common interests and goals seems like a productive and efficient practice, these collaborations may in fact be problematic.

Assembling heterogeneous organizations around a common goal requires communication and understanding on a greater level to ensure that the goal is not lost to misalignment of basic philosophies and strategic vision.[47] It has also been argued that because nonprofits are comprised of people and funders who fervently believe in their unique vision and mission, organizing efforts with other participants may be difficult. For example, if a collective impact initiative was assembled to stem teenage pregnancies, how could the parties who believe in birth control work effectively with those who advocate abstinence?[48] In addition, considering each organization's legal and fiduciary responsibilities to support ideas consistent with their missions and bylaws, ceding control to a larger group could disrupt participant groups and may even rise to legal action. Finally, in the event of a successful or failing effort, agreeing on how credit or blame is shared can possibly lead to further disputes.[49]

4. Evaluating Collaborative Efforts—The National Network of Fusion Centers Example

Irrespective of the type, or goal of any program, measurement and evaluation may be the most important component of any collaborative effort. Moreover, while true objective measurement can be elusive, it is incumbent upon each of the actors to agree upon a common set of metrics by which advances

[47] Emmett D. Carson, "Rethinking Collective Impact," August 31, 2012, http://www.huffingtonpost.com/emmett-d-carson/rethinking-collective-imp_b_1847839.html.

[48] Ibid.

[49] Ibid.

and successes can be measured.[50] When considering the implementation of performance assessment within the national network, an apparent paradox exists between the "top-down" strategic intent of the federal government and the "bottom up" reality of the state and local owners of the fusion centers themselves. Whereas, the top-down approach is a "centralized process that tends to neglect strategic initiatives coming from…other policy subsystems; bottom-up implementation is a decentralized process in which policy is determined by the bargaining between members of the organization and their clients."[51] It is also recognized that the key to implementing any performance management system is the organization's willingness to accept it.[52] An interesting example is the implementation of performance measures relating to the national network of fusion centers. Due to its unique composition, measuring the performance of the national network presented several challenges, most notably the following.

- *The diversity of the national network.* Since no two fusion centers are the same, performance measures that account for the diversity of the national network require the identification of common themes and approaches that apply to all or most fusion centers.

- *The diversity of fusion center customers*: Fusion centers must strike a balance between remaining relevant to their local area of responsibility and core customer set while supporting national priorities. Achieving this balance can be a daunting task since fusion centers are owned and operated by state and local governments whose priorities may be in conflict.

- *The intangible nature of the terrorism prevention mission area*: Measuring terrorism prevention is difficult; unless concrete evidence proves that the information provided by a fusion center led to the arrest of a potential terrorist, it is nearly impossible to

[50] *Government Performance and Results Act of 1993*, *An Act*, Pub. L. No. 103–62, 107 Stat. 285 (1993).

[51] Edward Long and Aimee L. Franklin, "The Paradox of Implementing the Government Performance and Results Act: Top-Down Direction for Bottom-Up Implementation," *Public Administration Review* 64, no. 3 (May–June 2004): 309–319.

[52] Michael J. Mucha, "Organizational Alignment with Logic Models," *Government Finance Review* 24, no. 5 (October 2008): 51–54.

> know if the cumulative actions of a fusion center, or group of centers, resulted in the prevention of a terrorist act.[53]

Recognizing these challenges, the DHS leveraged the logic model approach, which focuses more on an overall understanding of how program inputs translate into activities, outputs, and outcomes; from this basis program, measures are derived from indicators of success.[54] Additionally, the logic model captures the national network's operations at a high enough level to encompass most customer requirements, but with enough specificity to allow for the development of a full set of performance measures that capture the discrete functions of the national network.[55] A visual representation of the logic model as it applies to the national network in depicted in Figure 6.

[53] Department of Homeland Security, *Performance Measures Definition Guide*, ver. 1.0 (Washington, DC: Department of Homeland Security, April 2014), 6–7.

[54] Department of Homeland Security, *Performance Measures Definition Guide*, 6–7.

[55] Ibid.

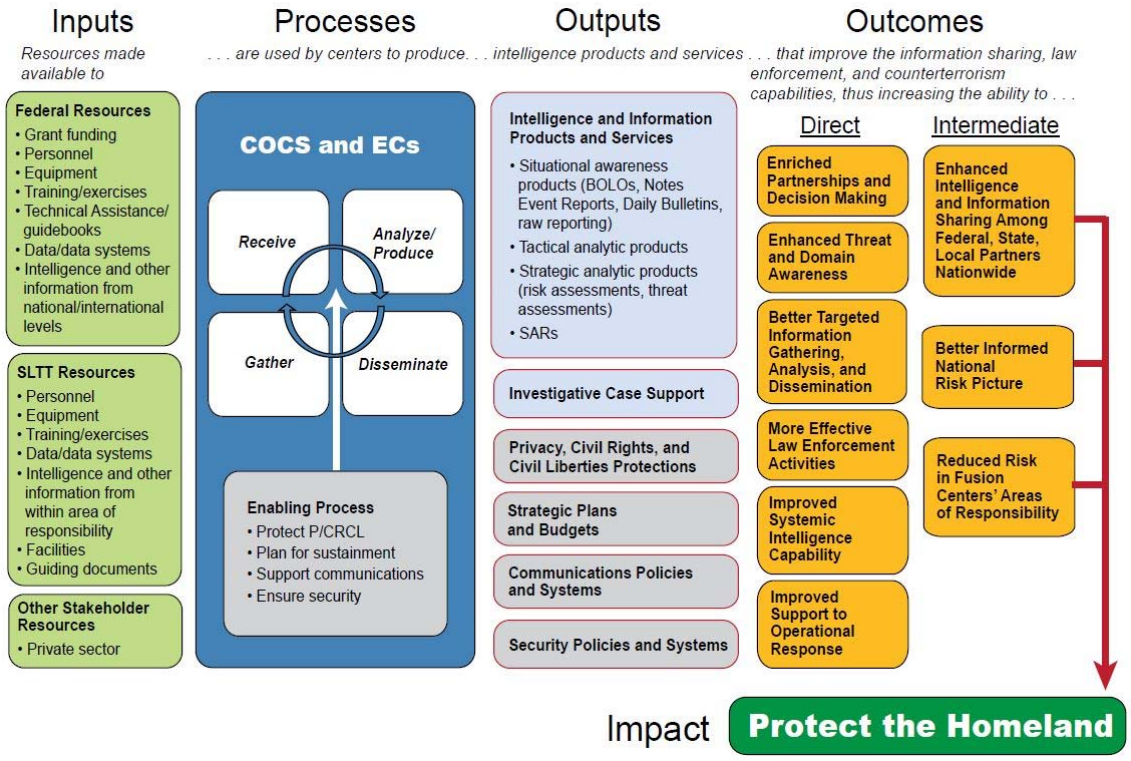

Figure 6. National Network Logic Model[56]

Beginning with the fusion center performance program (FCPP), the DHS, through its Office of Intelligence and Analysis (I&A), and State and Local Program Office (SLPO), began a program to "capture objective, standardized data to evaluate the value and impact of individual centers and the network as a whole."[57] The FCPP consisted of three interconnected elements.

- Measuring the capability and performance of the national network through a structured, standardized annual assessment
- Hosting and participating in prevention-based exercises that test fusion center capabilities against real world scenarios

[56] Department of Homeland Security, *2013 National Network of Fusion Centers Final Report* (Washington, DC: Department of Homeland Security, 2014), 4.

[57] Department of Homeland Security, *2013 National Network of Fusion Centers Final Report* 5.

- Mitigating identified gaps to increase capabilities, improve performance, and sustain fusion center operations[58]

Further defining the elements of the FCPP, in 2010, the DHS I&A, and members of the network identified four critical operational capabilities (COC), and four enabling capabilities (EC) that provide a foundation for the fusion process.[59] Using these eight criteria, baseline data relating to the performance of the national network was collected and reported in the *2012 Fusion Center Final Report*. This process was impactful because it provided a consistent measure of capability and maturity across a network of ostensibly dissimilar components. Another milestone in the evaluation of the national network is the release of the *2013 National Network of Fusion Centers Final Report* that builds on previous efforts. It is the first report on the national network that captures consistent year-over data, which lends to a more accurate indicator of real network progress. These performance measures are not, however, without debate. It can be argued that because of the intangible nature of the work with which fusion centers are tasked, and the subjective measure of some of the metrics, the capabilities and capacities captured by the assessment may merely be surrogates for qualitative impact.

C. CONCLUSION

Casual observation of the volume of reports related to the performance of government programs clearly indicate its importance to elected officials and the public alike. It follows that perhaps the most important feature of any collaboration is the proof of a partnership's impact, which also may be the most difficult feature to measure. The next three chapters illustrate how current intra-organizational efforts align closely with CI theory, although greater coordination between similar elements of the enterprise could provide greater results.

[58] Ibid.

[59] Ibid., 6.

III. REGIONAL INFORMATION SHARING CENTERS

A Proven Resource for Law Enforcement

–RISS motto

Perhaps the first formalized, multi-jurisdictional collaborative effort established between law enforcement agencies was the Regional Organized Crime Information Center (ROCIC). Formed over 40 years ago, and still in operation today, the ROCIC was the first of six RISS, and was founded with the understanding that criminals do not respect jurisdictional boundaries, and often travel to commit crimes. Further, realizing that an unmet need existed in sharing information across jurisdictions, agency representatives from several states met to discuss how they could better address common criminal issues. The establishment of the ROCIC became a catalyst for similar regional centers across the United States, which ultimately enabled the sharing of criminal intelligence, officer safety, and other public safety related information—both nationwide and internationally—seamlessly across its technology infrastructure.

A. HISTORY AND ESTABLISHMENT

In the late 1960s, and continuing through the early 1990s, several states across the southern United States were experiencing a significant problem with organized crime. Groups of traveling criminals known as the Dixie Mafia were engaged in high-profit burglaries, illegal gambling, prostitution, drugs, and the transportation of illegal alcohol and stolen property. Unlike other organized crime groups, the Dixie Mafia were not organized as traditional organized crime. In other words, no familial or hierarchical structure existed, which made targeting leadership and dismantling the groups much more difficult. Further complicating the investigation was that the groups of offenders were highly mobile and committed their crimes in many states across the southern United States. While these groups began by committing lower-level crimes, they became involved in

increasingly violent crimes, such as murder-for-hire and engaged in acts of violence in an effort to control territory. In addition, following a rash of 25 contract killings over six states, 23 senior law enforcement officials from 18 agencies met in New Orleans to discuss how they could better share information and coordinate their efforts.[60] Following the first meeting in New Orleans, quarterly meetings were held in Atlanta, and ultimately, the first of the RISS center's ROCIC was established in 1973, which was funded by the Law Enforcement Assistance Administration under the *Omnibus Crime Control and Safe Streets Act of 1968*.[61] Since the formation of ROCIC, five other RISS programs have been established, each with the initial charge to combat a specific criminal trend in their respective region. See Figure 7 for a map of each project's area of responsibility.

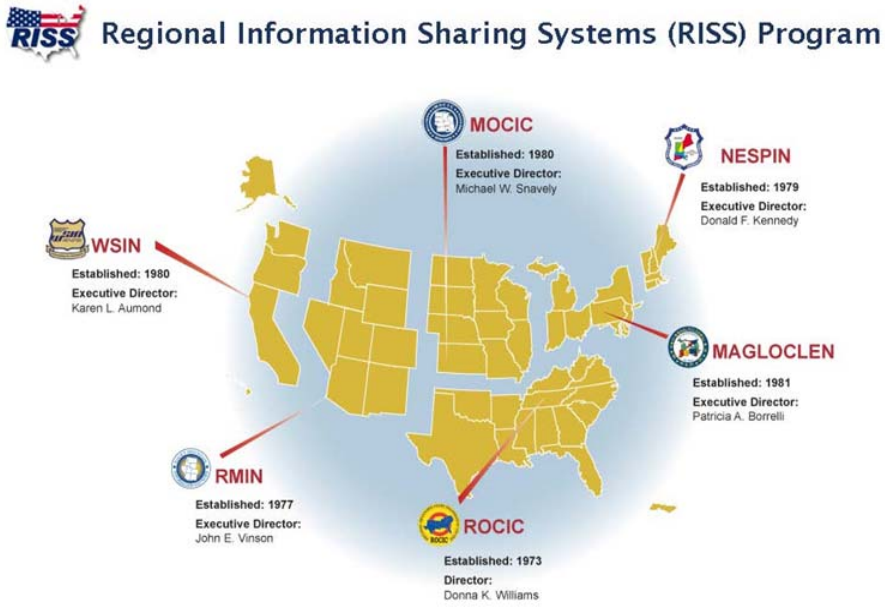

Figure 7. RISS Centers Map[62]

[60] ROCIC Mississippi Law Enforcement Coordinator, interview with author, July 7, 2014.

[61] *Report to the Chairman, Subcommittee on Commerce, Justice, State, and the Judiciary Committee on Appropriations, United States Senate, Regional Information Sharing Systems*, (GAO/GGD-85-17) (Washington, DC: General Accounting Office, 1984).

[62] Regional Information Sharing Systems, *Regional Information Sharing Systems Annual Report* (Washington, DC: Regional Information Sharing Systems, 2013), 2.

Each of the project's area of responsibility is discussed as follows.

- *Rocky Mountain Information Network* (RMIN)—Established in 1977, the RMIN was established to combat narcotics smuggling across the U.S.-Mexican border in four southern counties of Arizona.

- *New England State Police Information Network* (NESPIN)—Established in 1979, NESPIN first focused on organized crime in the New England states and grew its mission to support narcotics smuggling and distribution. It serves not only the northeastern United States, but areas of Canada as well.

- *Mid-States Organized Crime Information Center* (MOCIC)—In 1980, traveling criminals were committing burglaries in several states in the Midwest. MOCIC was organized so that several jurisdictions could collaborate on case information.

- *Western States Information Network (WSIN)*—In 1980, the WSIN was organized to support major investigations involving narcotics smuggling and distribution in California and several the Pacific Rim states.

- *Middle Atlantic Great Lakes Organized Crime Law Enforcement Network* (MAGLOCLEN)—Established in 1981, the last of the regional centers to form was the MAGLOCLEN. It was established primarily to fight "traditional" organized crime in the northeastern and most densely populated part of the country.[63]

B. STATED MISSION AND PRIMARY ACTIVITIES

While each of the RISS centers was formed to combat a specific issue, the centers realized that several law enforcement agencies in their area of responsibility lacked specific capability and could benefit from enhanced services from their center.[64] The mission of the centers expanded quickly and the centers began to provide their member agencies with a number of services, including the following.

- *Information sharing*—Perhaps the most frequently used service provided by RISS is its web-based technology platform, or

[63] Regional Information Sharing Systems, *Regional Information Sharing Systems Program History and Evolution* (Washington, DC: Regional Information Sharing Systems, 2013).

[64] ROCIC Mississippi Law Enforcement Coordinator, interview with author.

RISSNET™, which provides a secure environment for sharing sensitive but unclassified[65] information with appropriately vetted individuals.

- *Analysis*—RISS centers employ analysts to assist member agencies in the compilation and analysis of data, computer forensics, and preparation of visual materials to aid prosecution. These analysts also monitor criminal trends in their region and across the nation, and prepare information bulletins, reference guides, and other intelligence products for member agencies.

- *Equipment Loans*—Inventories of specialized investigative and surveillance equipment, including photographic, communications, and surveillance equipment is available for member agencies to borrow for multijurisdictional investigations.

- *Confidential Funds*—Following federal and RISS center guidelines, funds are provided by each center that can be used to purchase information, contraband, stolen property, and other evidentiary items, as well as to pay investigative expenses for multijurisdictional investigations.

- *Training*—The RISS program supports meetings and conferences on emerging issues and criminal trends, and information-sharing and analytical techniques.

- *Technical Assistance*—Member agencies can request training and assistance for activities, such as intelligence analysis and installation of specialized equipment.[66]

- *Event Deconfliction*—In the interest of increasing officer safety by disambiguation, the RISS program supports a technology solution called RISSafe. This technology allows member agencies to add planned enforcement activity (i.e., surveillance, search warrants, and the presence of undercover officers) into a common database with the goal of reducing "blue on blue"[67] incidents.

---

[65] Sensitive but unclassified (SBU) information is commonly referred to as information not classified for national security reasons, but that warrants/requires administrative control and protection from public or other unauthorized disclosure for other reasons.

[66] Harold C. Relyea and Jeffrey W. Seifert, *Information Sharing for Homeland Security: A Brief Overview* (CRS Order Code RL32597) (Washington, DC: Congressional Research Service, 2005).

[67] Blue on blue incidents are commonly defined as direct action against friendly forces who are misidentified as threats.

C. ORGANIZATION AND FUNDING

The DOJ's Bureau of Justice Assistance (BJA) congressionally funds the RISS program through grant awards.[68] Moreover, although the funding is provided to the RISS program as the larger entity, funds are divided between centers by the RISS National Policy Group (RNPG). Heading the RNPG is the national coordinator who is responsible for the operation of the RISS program at the enterprise level. Additionally, the national coordinator is responsible for ensuring that program objectives are met and new opportunities to promote RISS initiatives are capitalized upon and identified. The RNPG is comprised of the directors of each RISS center along with the chair of each center's policy board. This group makes determinations relating to strategic planning, resolution of operational issues, advancement of information-sharing initiatives, and other issues regarding the nationwide operation of the program. In addition, each RISS center has a policy board that is comprised of representatives from member agencies in the center's multi-state region along with the in-region director. Regional policy boards serve as the governing body for each of the individual centers and make determinations relating to regional administration, strategy, and implementation of national directives.[69]

D. HOW RISS MEASURES ITS EFFECTIVENESS

RISS maintains a comprehensive performance plan and reports and analyzes performance on a regular basis. Program effectiveness is measured by the delivery and acceptance of RISS reports, data analysis, educational products, policy documents, strategic plans, performance measures, and feedback from RISS center management and staff and the BJA program office.[70]

---

[68] "Frequently Asked Questions, How is RISS Funded?," Regional Information Sharing Systems, accessed July 15, 2014, http://www.riss.net/default/faq#7.

[69] "Regional Information Sharing Systems (RISS) Program," Regional Information Sharing Systems, accessed July 15, 2014, https://www.riss.net/default/Overview.

[70] "Frequently Asked Questions," Regional Information Sharing Systems, accessed July 14, 2014, https://www.riss.net/Documents/RISS.FAQ.pdf.

In addition, an executive summary is produced that provides the following information.

- Number of member agencies and authorized users
- Seizures, recoveries, and arrests as a result of RISS sponsored services
- Summary of investigative support services
- Field service activities
- Use of RISSNET™ resources
- Database records available via RISSNET™
- Inquiries to RISS sources
- Hits to RISS sources
- Number of events deconflicted through RISSafe[71]

E. RISS AND COLLECTIVE IMPACT

Due to their original and enduring mandates to enhance collaboration and information sharing among law enforcement agencies, it could be argued that the activities of RISS centers show indications of working within the CI framework. However, one important point to note is that the effectiveness of RISS centers as a stand-alone entity would be limited without the participation of a secondary network of local, state, federal, and tribal member agencies. The result is a three-tier network, which supports both the needs of individual members and the larger goals of the national program. Considering the framework of CI, a lot evidence is available to support how RISS centers have embraced the basic elements of CI, more specifically as follows.

[71] "Frequently Asked Questions."

1. Common Agenda

Beginning with the formation of the first RISS center some 40 years ago, and continuing to present day operations, RISS centers have engaged their membership with the foundational agenda of collaboration and information sharing. In addition to the underlying goal of fostering information sharing, sub-agendas that are topical in nature have developed with the intent to provide stakeholders with access to a wider variety of sources. Such is the case with the development of the RISSGang™ and RISS' automated trusted information exchange, or ATIX™. RISSGang™ provides users with federated access to several state, local, and federal criminal gang databases,[72] and ATIX™ is a platform on which law enforcement, public safety, and private sector communities can share disaster, terrorism, and homeland security information.[73] Both these information-sharing services support the common agenda of increasing the reach of information shared across appropriate audiences.

2. Shared Measurement

Measurement of the effectiveness of the RISS program is expressed in two separate, but equally important ways, empirically through the volume of work completed and through success stories. Internal to the network of RISS centers is a set of criteria that illustrates empirically how the network of RISS centers executes its core mission and provides value to its member agencies. While most these areas of measurement are more indicative of the volume of work rather than impact, RISS centers do track arrests, seizures, and forfeitures arising from the assistance they provide. RISS centers also capture success stories and testimonials, which demonstrate the effectiveness of the system.

---

[72] Regional Information Sharing Systems, *Regional Information Sharing Systems Annual Report, RISSGang Brochure* (Washington, DC: Regional Information Sharing Systems, 2013), 11.

[73] Regional Information Sharing Systems, *Regional Information Sharing Systems Annual Report, ATIX Brochure* (Washington, DC: Regional Information Sharing Systems, 2013), 11.

3. Mutually Reinforcing Activities

Information sharing in and of itself could be construed as a mutually reinforcing activity in which all the members of the community have some responsibility to share information they have in exchange for other members' data. The number of transactions recorded by the RISS automated systems easily proves this activity. In addition, while numerous information-sharing initiatives are in existence, which are mostly topical in nature, perhaps the most consequential information-sharing effort is the event deconfliction tool provided by RISS, named RISSafe™. In 2013, nearly 180,000 events were submitted for deconfliction into the RISSafe™ system, with over 73,000 conflicts identified.[74] This activity is deemed so important that California law now requires law enforcement agencies to enter enforcement activities into an event deconfliction system.

4. Continuous Communication

In addition to supporting several information-sharing tools and platforms, RISS centers offer training and networking opportunities through a variety of training courses, seminars, and conferences. These in-person events, usually held three times per year in each region, allow participants to open and maintain lines of communication both within their network and among their member agencies. Additionally, the RISS project employs law enforcement coordinators whose sole purpose is to build relationships with new collaborative partners. In support of this mission area, RISS field service representatives conducted over 20,000 onsite visits with prospective and member agencies across the country.[75]

---

[74] Regional Information Sharing Systems, *Regional Information Sharing Systems Annual Report, Executive Summary* (Washington, DC: Regional Information Sharing Systems, 2013).

[75] Regional Information Sharing Systems, *Regional Information Sharing Systems Annual Report, Executive Summary*.

5. Backbone Support

RISS centers' primarily receive backbone support from the DOJ and the Institute for Intergovernmental Research (IIR). Whereas the DOJ provides funding to sustain the operation of the six RISS centers and the RISS technology support center, IIR provides the RISS centers with technical services related to ongoing training, project coordination, research, performance measurement and evaluation, and analysis of the program.[76]

F. CONCLUSION

It is easy to see that in the 40 years since their establishment, RISS centers have validated the core concepts and effectiveness of CI. However, this begs the question; must collaboration be framed, or is it more successful when it forms organically from an unmet need? One thing is clear in the case of the first RISS center. Similarly, interested groups who need to solve complex problems seem to unite in pursuit of common goals, even before a formal framework is established.

Further, it could be confidently asserted that the first RISS center, ROCIC, grew organically to satisfy a previously unidentified and unmet need. Moreover, while strong ties exist among and between the six RISS centers, it could be argued that they remain somewhat isolated by their backbone organization and segregated information-sharing platform.

[76] "Regional Information Sharing Systems (RISS)," Institute for Intergovernmental Research, July 15, 2014, https://www.iir.com/WhatWeDo/Information_Sharing/RISS/.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. HIGH INTENSITY DRUG TRAFFICKING AREA INVESTIGATIVE SUPPORT CENTERS

Reducing the Threat by Addressing the Flow

–Gulf Coast HIDTA motto

As a key partner in the domestic intelligence enterprise, HIDTA ISCs provide valuable counterdrug intelligence to policy makers, investigators, and law enforcement leaders. Also, because it is recognized that a clear link exists between crimes associated with drug trafficking and terrorism, and in many cases, narcotics-related crimes either provide finance or are precursors to terrorism, this intelligence is important to larger homeland security efforts.[77] In addition, ISCs deliver strategic and tactical intelligence products in an effort to better inform the decisions of law enforcement leaders, which can ultimately lead to enhanced officer safety, more effective investigative strategy, and more efficient resource allocation. This chapter reviews the history of these centers, and argues that they are successful largely because they follow the principles of CI.

A. HISTORY AND ESTABLISHMENT

Declaring that illicit drugs were a threat to U.S. national security, in 1986, President Ronald Reagan issued National Security Decision Directive 221, which, among other things, established the intelligence community as a key partner in the fight against illicit drugs. In addition, on November 18, 1988, President Reagan signed the *Anti-Drug Abuse Act of 1988*, which created the Office of National Drug Control Policy to coordinate drug-related legislation,

[77] "Fusion Centers and HIDTA Investigative Support Centers," Department of Homeland Security, accessed June 26, 2014, http://www.dhs.gov/fusion-centers-and-hidta-investigative-support-centers.

security, diplomatic, research and health policy throughout the government.[78] With the passage of the *Anti-Drug Abuse Act of 1988* and the *ONDCP Reauthorization Act of 1998*, the ONDCP director was authorized to designate areas within the United States that exhibit serious drug trafficking problems as HIDTA, or areas.[79]

The HIDTA program provides additional federal resources to those areas to help eliminate or reduce drug trafficking and its harmful consequences. Law enforcement organizations within HIDTAs assess drug trafficking problems and design specific initiatives to reduce or eliminate the production, manufacture, transportation, distribution, and chronic use of illegal drugs and money laundering.[80] The reach and coverage of HIDTA is significant. Twenty-eight areas have been designated across the United States and its territories (as indicated in Figure 8), while nearly 15 percent of all counties and 58 percent of the U.S.' population are included in a HIDTA.[81]

[78] *Anti-Drug Abuse Act of 1988*, Pub. L. 100–690, 102 Stat. 4181 (1988).

[79] Executive Office of the President, *National Drug Control Strategy* (Washington, DC: HIDTA, Office of National Drug Control Policy, 2004).

[80] "High Intensity Drug Trafficking Areas (HIDTA) Program," The White House, Office of National Drug Control Policy, accessed May 1, 2014, http://www.whitehouse.gov/ondcp/high-intensity-drug-trafficking-areas-program.

[81] "Fusion Centers and HIDTA Investigative Support Centers."

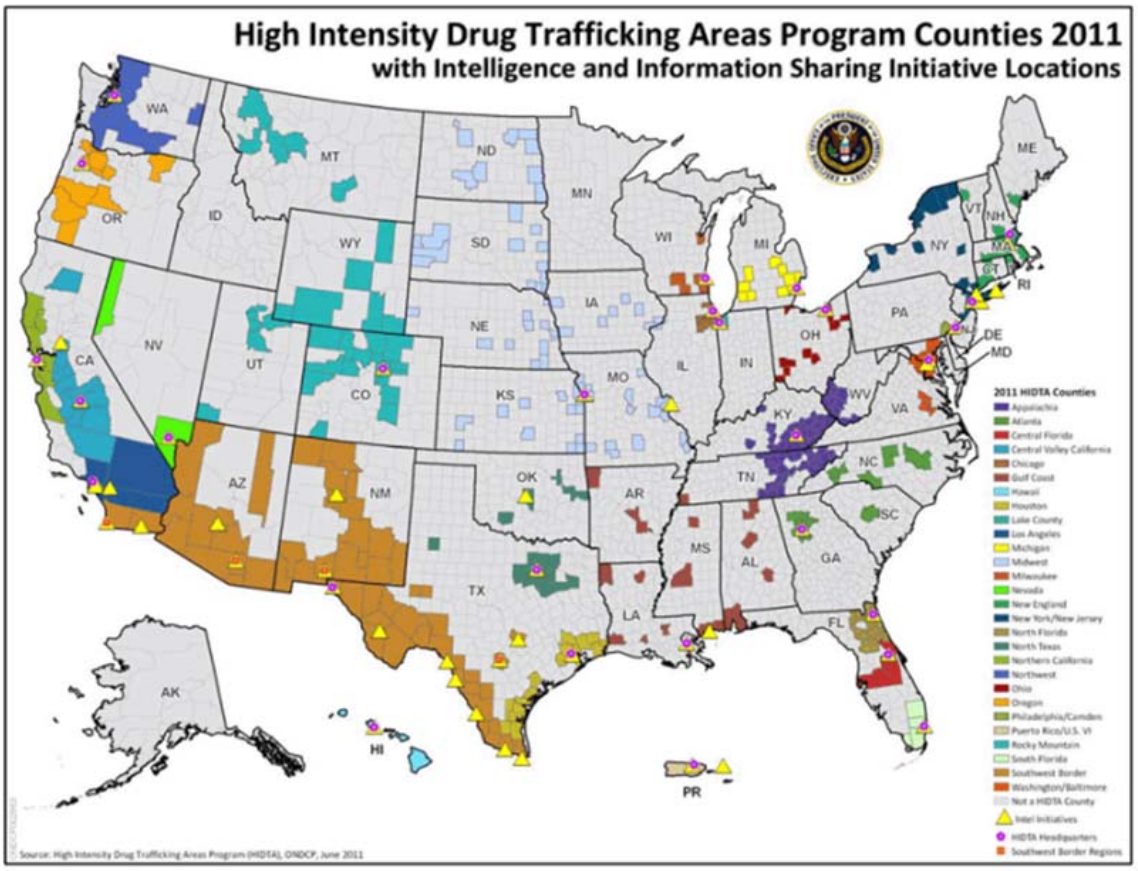

Figure 8. HIDTA Regions and ISC Locations[82]

B. STATED MISSION AND PRIMARY ACTIVITIES

Accompanying the additional enforcement resources, HIDTA programs bring to an area is an intelligence and case support function known as the ISC. In addition to investigative support, ISCs are intended to better inform and focus enforcement operations and enhance officer safety. The objective of the HIDTA ISC is two-fold.

- Provide actionable, accurate, detailed, and timely drug and criminal intelligence, information, and analytical support to HIDTA enforcement initiatives, HIDTA participating agencies, and to other law enforcement agencies and intelligence centers

82 "Fusion Centers and HIDTA Investigative Support Centers."

- Collect, collate, analyze, and disseminate information about offenders, crimes, and/or events to law enforcement agencies[83]

The above objectives are executed through five specific functions, which include the following.

- *Analytical Services*—Analytical tradecraft performed by an analyst to support an investigation, and includes association/link/network analysis, commodity flow analysis, crime-pattern analysis, financial analysis, or flow analysis.

- *Threat Assessments*—Each HIDTA is required to publish an annual threat assessment that documents the drug trafficking in its region. In addition, ISCs produce other topical assessments as necessary.

- *Intelligence Products*—ISCs are responsible for producing tactical operational, and strategic intelligence products.

- *Information Sharing*—ISCs should ensure that drug-related information is shared from law enforcement, proprietary, and public databases with other ISCs, national intelligence centers (e.g., El Paso Intelligence Center (EPIC) and Financial Crimes Enforcement Network (FinCEN)), and fusion centers.

- *Deconfliction*—ISCs are required to establish a mechanism to perform target, case, and event disambiguation.[84]

In addition, the ISC is envisioned as a mechanism by, and through which, agencies communicate more rapidly and effectively and share intelligence resources, with the larger goal of building a common vision and collective problem solving techniques.[85]

---

[83] Office of National Drug Control Policy, "Intelligence and Information Sharing," in *Program Policy and Budget Guidance* (Washington, DC: Executive Office of the White Office, 2009), sec. 5.0, 5–1—5–6.

[84] Ibid.

[85] Quoted from NPS thesis, Michael J. Gutierrez, "Intelligence and High Intensity Drug Trafficking Areas (HIDTA'S): A Critical Evaluation of the HIDTA Investigative Support Center" (master's thesis, Naval Postgraduate School, 2004), 11.

C. ORGANIZATION AND FUNDING

Each HIDTA is funded individually by a grant from the ONDCP and governed by its own local executive board, typically consisting of 16 members with half of the members coming from state and local agencies. While the purpose of the local boards is to ensure that federal priorities are carried through, a great amount of discretion is granted to ensure that issues unique to the local community are addressed in the overall strategy for that HIDTA. Local control is reinforced by each executive board's ability to design and implement its own strategy, along with the flexibility to adjust tactics to meet changing conditions.[86] Funding for calendar year 2012 was approximately $238.5 million, and included salaries for nearly 1,200 positions.[87]

D. HOW HIDTA MEASURES ITS EFFECTIVENESS

In 2003, the Executive Office of the President, along with the DOJ published the newly developed *Design for a HIDTA/OCDETF Performance Monitoring and Management System.* The project's focus was to first, identify law-enforcement program measures specifically relevant to HIDTA (and Organized Crime Drug Enforcement Task Forces (OCDETF)), and second, to recommend a method for implementing a management and reporting system for the two programs.[88] The new evaluation regime is based on a logic model[89]

---

[86] Office of National Drug Control Policy, *HIDTA Program Policy and Budget Guidance* (Washington, DC: Executive Office of the White House, 2012).

[87] National HIDTA Directors Association, *HIDTA Program Summary 2012* (Alexandria, VA: National HIDTA Directors Association, 2012).

[88] Office of National Drug Control Policy, *Design for a HIDTA/OCDETF Performance Monitoring and Management System* (Washington, DC: Executive Office of the White House, 2003).

[89] A logic model is a planning tool to clarify and graphically display what your project intends to do and what it hopes to accomplish and impact. "Guide 5: Define How a Program Will Work—The Logi Model," National Network of Libraries of Medicine, last updated October 5, 2012, nnlm.gov/outreach/community/logicmodel.html.

(depicted in Figure 9), which seeks the ultimate impact of reduced availability of illegal narcotics.[90]

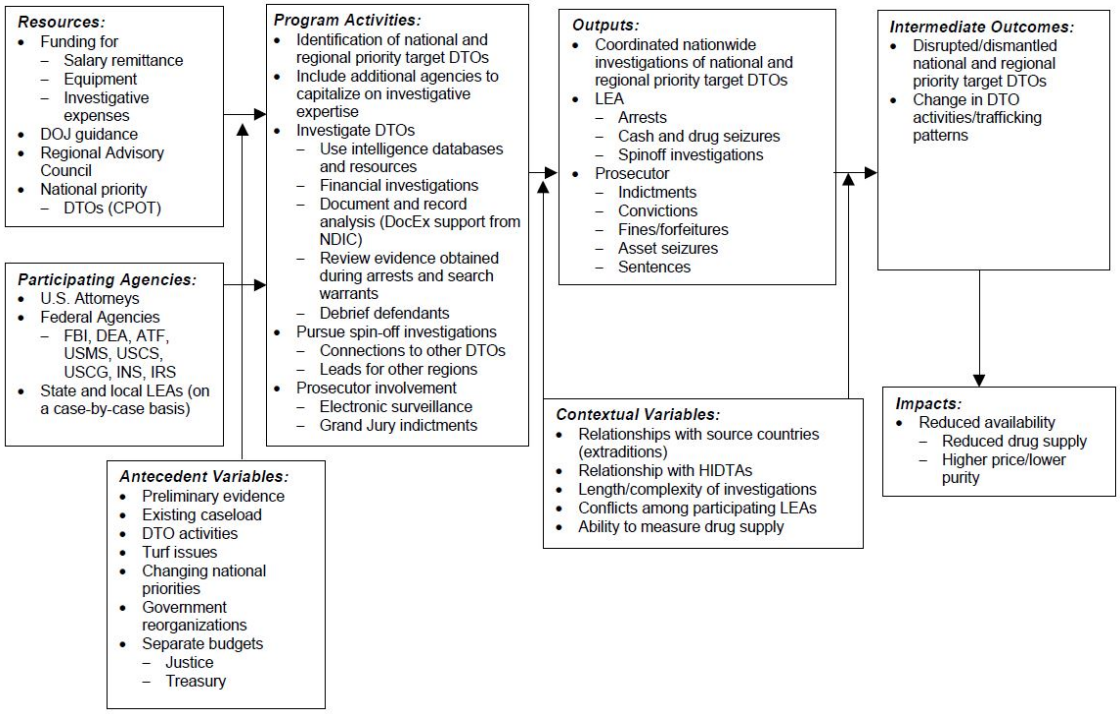

Figure 9. HIDTA Logic Model[91]

Notwithstanding the logic model and other measures of performance mentioned previously, the HIDTA program measures its impact primarily through quantitative statistics, more specifically the following.

- Arrests related to HIDTA supported investigations
- Seizures of illegally obtained assets
- The quantity of leads processed and investigations supported

[90] Office of National Drug Control Policy, *Design for a HIDTA/OCDETF Performance Monitoring and Management System*.

[91] Office of National Drug Control Policy, *Design for a HIDTA/OCDETF Performance Monitoring and Management System*, 37.

- The number of drug trafficking organizations disrupted or dismantled[92]

Albeit limited in scope, another project that sought to evaluate the performance of the ISC was published in 2009. Titled *Using SERVQUAL to Assess the Customer Satisfaction Level of the Oregon HIDTA ISC Analytical Unit*, the report leveraged SERVQUAL, which is a multi-item scale developed to assess perceptions of service quality in service and retail businesses. Among the dimensions collected were the following.

- *Tangibles*—Physical facilities, equipment, staff appearance, etc.
- *Reliability*—Ability to perform service dependably and accurately
- *Responsiveness*—Willingness to respond to customer need
- *Assurance*—Ability of staff to inspire confidence and trust
- *Empathy*—The extent to which caring individualized service is given[93]

This limited study found that, in general, customers (meaning personnel using the ISC) were largely satisfied with the services provided by the Oregon HIDTA ISC.

E. HIDTA ISCS AND COLLECTIVE IMPACT

- Common Agenda–The common agenda binding HIDTAs, their associated ISCs, and existing local resources is the idea that the narcotics issue in the United States cannot be addressed by the individual actions of state, local, and federal agencies working individually. Rather, the HIDTA program provides additional resources to address the problem; among the most important are funding, personnel and information.
- Shared Measurement–Both through the threat assessment process and the reporting of case statistics, each of the HIDTA ISCs

[92] National HIDTA Directors Association, *HIDTA Program Summary 2012*.

[93] Chris Gibson, *Using SERVQUAL to Assess the Customer Satisfaction Level of the Oregon HIDTA ISC Analytical Unit* (Portland, OR: Hartfield School of Management, Portland State University, 2009).

contribute to a consistent enterprise-wide measure of the work it is doing and how expenditures are either making the intended impact, or why efforts might have been hampered. As mentioned previously, measures of impact are largely quantitative, and limited attempts have focused on the operation of the enterprise rather than the impact of the designated mission.

- Mutually Reinforcing Activities–Their common mission binds the network of HIDTAs and their accompanying ISCs across the nation. Additionally, intelligence components reinforce the efforts of the entire network and provide guidance via empirical data to guide both the activities of field personnel and future policy.

- Continuous Communication–Empirical data indicate that ISCs are in constant communication both internally and throughout the network. For example, in 2012, over 50,000 leads were referred and over 240,000 events were deconflicted.

- Backbone Support–The backbone support for the network of HIDTA ISCs comes from the ONDCP primarily through funding and additional personnel. The ONDCP also provides guidance for programmatic activities via its national drug control strategy while local boards direct the priorities of individual centers as deemed by their leadership.

F. CONCLUSION

Similar to the example of the RISS centers, HIDTA ISCs exhibit strong alignment with the principles proposed by collective impact. Moreover, even though their formation was compelled by statute and not by a natural need to collaborate, the HIDTA intelligence system, or ISC, has been described as "an indispensable element in the creation and growth of numerous local, state, and federal intelligence programs."[94]

[94] Kurt Schmid, "A Foundation for Information Sharing," *Police Chief Magazine* 70, no. 11 (November 2003).

V. NATIONAL NETWORK OF FUSION CENTERS

Homeland security begins with hometown security, and fusion centers play a vital role in keeping communities safe all across America

—Janet Napolitano

The most recent and perhaps most controversial addition to the domestic intelligence enterprise is the National Network of Fusion Centers (NNFC) Comprised of 78 individual centers located in 49 U.S. states and two territories,[95] the NNFC is ostensibly the nation's solution for enhancing information-gathering and sharing activities on the state and local level to inform the national threat picture. Conversely, the NNFC aims to keep state and local entities informed of transnational threats, which may have nexus to their community.

A. HISTORY AND ESTABLISHMENT

Following the intelligence and information-sharing failures leading up to the September 11, 2001, terrorist attacks on the United States, the U.S. government began the process of studying the issue and recommended both legal and organizational solutions. From 2002–2012, no fewer than eight reports[96] were published that recommended and guided possible solutions. Included in these reports was the *9/11 Commission Report*, published in 2002, which recommended that information be shared across a wider audience of stakeholders and across new networks.[97]

---

[95] The state of Wyoming does not have a designated fusion center; and Guam and Puerto Rico both have centers.

[96] These reports included, *The 9/11 Commission Report* (2002), *The National Criminal Intelligence Sharing Plan* (2003), *The Intelligence Reform and Terrorism Prevention Act* (2004), *The Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* (2005), *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (2006), *National Strategy for Information Sharing, Success and Challenges in Improving Terrorism-Related Information Sharing* (2007), *Enabling Capabilities for State and Major Urban Area Fusion Centers* (2008), *The National Strategy for Information Sharing and Safeguarding* (2012).

[97] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: U.S. Government Printing Office), 418.

The theme of information sharing for law enforcement was given a concrete framework and course of action in the National Criminal Intelligence Sharing Plan (NISCP), which was published in 2003. The plan, which was not developed solely for fusion centers, arose from the collaboration of the Global Intelligence Working Group, which was formed following the 2002 International Association of Chiefs of Police Criminal Information Sharing Summit. The vision of the working group was to create the following

- A model intelligence sharing plan
- A mechanism to promote intelligence-led policing
- A blueprint for law enforcement administrators to follow when enhancing or building an intelligence system
- A model for intelligence process principles and policies
- A plan that respects and protects individuals' privacy and civil rights
- A technology architecture to provide secure, seamless sharing of information among systems
- A national model for intelligence training
- An outreach plan to promote timely and credible intelligence sharing
- A plan that leverages existing systems and networks, yet allows flexibility for technology and process enhancements[98]

Further defining information-sharing protocols, procedures and expectations was the IRTPA. The IRTPA called for the creation of the ISE, and with relation to the national network of fusion centers, the requirement that the ISE will provide and facilitate "the means for sharing terrorism information among

[98] Department of Justice, *National Criminal Intelligence Sharing Plan* (Washington, DC: Department of Justice, 2003).

all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies."[99]

In 2005, the DHS's Homeland Security Advisory Council issued a document titled *Intelligence and Information Sharing Initiative: Homeland Security and Intelligence Fusion*. This document identified that the concept of intelligence/information fusion has emerged as the fundamental process to facilitate the sharing of homeland security-related information at a national level, and therefore, has become a guiding principle in defining the ISE (as required by the IRTPA of 2004).[100] The document identified the priorities of homeland security intelligence/information as efforts to do the following.

- Identify rapidly both immediate and long-term threats
- Identify persons involved in terrorism-related activities
- Guide the implementation of information-driven and risk-based prevention, response, and consequence management efforts[101]

The document further defined the following, which could ostensibly be considered an early roadmap to fusion center standards.

- How homeland security intelligence/information fusion is the overarching process of managing the flow of information and intelligence across levels and sectors of government, and the private sector to support the rapid identification of emerging terrorism-related threats and other circumstances requiring intervention by government and private sector entities.

[99] Quoted from the National Strategy for the National Network of Fusion Centers, Department of Homeland Security, *National Strategy for the National Network of Fusion Centers* (Washington, DC: Department of Homeland Security, 2014).

[100] Homeland Security Advisory Council, "Intelligence and Information Sharing Initiative, Homeland Security Intelligence & Information Fusion," Department of Homeland Security, April 2005, http://www.dhs.gov/xlibrary/assets/HSAC_HSIntelInfoFusion_Apr05.pdf.

[101] Ibid.

- The importance of involving every level and discipline of government, the private sector and the public, and how efforts should be organized in a scalable way and on a geographic basis so that adjustments can be made based on the operating and/or threat environment.

- A description of the fusion process that includes the following activities and could arguably be the predecessor to the intelligence cycle adopted by the national network.

    - Management and governance
    - Planning and requirements development
    - Collection
    - Analysis
    - Dissemination, tasking, and archiving
    - Reevaluation
    - Modification of requirements[102]

A further definition of the operation of fusion centers was contained in a 2006 publication titled *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era.* The intent of this document was not to dictate the emphasis or priorities of individual centers; rather, it was to provide newly organized fusion centers with standards and guidelines for operation, as well as advice for the effective exchange of information throughout the network. Three phases of development (Phase 1—Law Enforcement Intelligence Component, Phase 2—Public Safety Component, and Phase 3—Private Sector Component) were accompanied by 18 guidelines that were developed to clarify the standards for the successful operation of a single center and assist with the development of the NNFC. Those guidelines, each with an accompanying instructional document, are listed as follows.

[102] Homeland Security Advisory Council, "Intelligence and Information Sharing Initiative."

Guideline 1: The NCISP and the Intelligence and Fusion Processes

Guideline 2: Mission Statement and Goals

Guideline 3: Governance

Guideline 4: Collaboration

Guideline 5: Memorandum of Understanding and Non-Disclosure Agreement

Guideline 6: Database Resources

Guideline 7: Interconnectivity

Guideline 8: Privacy and Civil Liberties

Guideline 9: Security

Guideline 10: Facility, Location, and Physical Infrastructure

Guideline 11: Human Resources

Guideline 12: Training of Center Personnel

Guideline 13: Multidisciplinary Awareness and Education

Guideline 14: Intelligence Services and Products

Guideline 15: Policies and Procedures

Guideline 16: Center Performance Measures

Guideline 17: Funding

Guideline 18: Communications Plan[103]

In 2007, the *National Strategy for Information Sharing* identified state, local and tribal entities as "full and trusted partners with the federal government in our nation's efforts to combat terrorism."[104] The document identified three areas in which federal departments and agencies could better coordinate efforts with their state, local, and tribal counterparts, and also introduced, without naming it specifically, the concept of sharing information in an all-crimes, all-hazards environment. The document mentioned activities, which would enhance information sharing, more specifically emphasize the following.

[103] Department of Justice, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (Washington, DC: Department of Justice, 2006).

[104] The White House, *National Strategy for Information Sharing, Success and Challenges in Improving Terrorism-Related Information Sharing*).

- Foster a culture that recognizes the importance of fusing information regarding all crimes with national security implications, with other security-related information (e.g., criminal investigations, terrorism, public health and safety, and natural hazard emergency response)

- Support efforts to detect and prevent terrorist attacks by maintaining situational awareness of threats, alerts, and warnings, and develop critical infrastructure protection plans to ensure the security and resilience of infrastructure operations (e.g., electric power, transportation, telecommunications) within a region, state, or locality

- Develop training, awareness, and exercise programs to ensure that state, local, and tribal personnel are prepared to deal with terrorist strategies, tactics, capabilities, and intentions, and to test plans for preventing, preparing for, mitigating the effects of, and responding to events[105]

In 2008 and 2012, the fusion centers' role was further refined and defined by the publication of *Baseline Capabilities for State and Major Urban Area Fusion Centers*, and the updated *National Strategy for Information Sharing and Safeguarding*. In these documents, the further development of expertise within the NNFC is encouraged and the Network is again identified as a critical partner in the collection and analysis of threat-related information.

With the exception of Wyoming, each state has at least one fusion center, and several states have multiple fusion centers, which may be missioned to support specific local agencies or to provide analytical support on certain issues. While the fusion center concept is not new,[106] centers following the homeland security model began organizing in 2002, growing to 29 in the year 2005, and more than doubling in 2007 to sixty.[107] The number currently stands at 78, with centers in both Guam and Puerto Rico.

---

[105] The White House, *National Strategy for Information Sharing, Success and Challenges in Improving Terrorism-Related Information Sharing*.

[106] The New York City Police Department had a system in place in the 1990s to ensure information was shared between the detective, patrol, and organized crime sections.

[107] Department of Homeland Security, *2013 National Network of Fusion Centers Final Report*.

Figure 10. Map of DHS Designated Fusion Centers[108]

B. STATED MISSION AND PRIMARY ACTIVITIES

A common theme woven throughout several national-level documents is the idea that the principal activity of a fusion center is to facilitate the sharing of information. Recognizing the unique capabilities of its member centers, and emergent nature of the NNFC, the mission statement for the national network remains quite general in nature.

> The mission of the National Network is to use the capabilities unique to the NNFC and the state and major urban area fusion centers included in the National Network to receive, analyze, disseminate, and gather threat information and intelligence in support of state, local, tribal, territorial, private sector, and federal efforts to protect the homeland from criminal activities and events, including acts of terrorism.[109]

In addition, considering that many fusion centers have specific topical focus, it can be accurately stated that their primary goal is to enhance public

[108] Department of Homeland Security, *2013 National Network of Fusion Centers Final Report*.

[109] Department of Homeland Security, *National Strategy for the National Network of Fusion Centers*.

safety through the timely sharing of relevant information with the most appropriate audience.

C. ORGANIZATION AND FUNDING

The centers that comprise the Network are owned and operated by a variety of state and/or local government organizations, and therefore, are each organized in a unique way. Whereas some centers are operated by a state police agency with dedicated personnel, others function more like a task force with individuals from many agencies who are detailed to the center. It follows that the funding mechanism for each center is equally as unique.

Several federal funding sources are available to support the NNFC. The largest is the state homeland security grant program. In addition, the DOJ makes funding available through its Office of Community Oriented Policing Services and the Bureau of Justice Assistance. Funding can also be dependent upon the partners present, as funding and assistance is available from the Department of Health and Human Services for centers that include a public health element.

In recent years, and with the encouragement of the DHS, the NNFC has been urged to formulate operational sustainment plans, which rely less on federal dollars and more on state and local stakeholder funding. State and local sustainment has taken hold as evidenced in the reduced level of federal investment in fusion centers; in 2013, direct federal investment decreased by 10 percent, and in 13.3 percent in the previous year. In the years 2011 through 2013, direct federal investment declined by 28.5 percent.[110]

D. HOW THE NATIONAL NETWORK OF FUSION CENTERS MEASURES ITS EFFECTIVENESS

Beginning in 2010, and as a follow on to the document *Fusion Center Guidelines, the National Strategy for Information Sharing, the Baseline Capabilities for State and Major Urban Area Fusion Centers*, the Network sought

[110] Department of Homeland Security, *2013 National Network of Fusion Centers Final Report*.

to measure its progress in building capacity through FCPP, which consists of the following three activities.

- Measuring the capability and performance of the national network through a structured, standardized annual assessment
- Hosting and participating in prevention-based exercises that test fusion center capabilities against real-world scenarios
- Mitigating identified gaps to increase capabilities, improve performance, and sustain fusion center operations[111]

More focused on assessing the maturity level of the network, the FCPP collected data from each of the centers with respect to its progress in building core capabilities (described in more detail in subsequent sections).[112] The initial assessment process has since grown from a basic measure of capability, to a more robust assessment of performance. The *2013 National Network of Fusion Centers Final Report*, released in June 2014, represents the third iteration of a repeatable annual assessment process with objective and standardized data to measure year-over-year progress.[113]

E. COLLECTIVE IMPACT AND THE NATIONAL NETWORK OF FUSION CENTERS

1. Common Agenda

Apart and aside from its mission statement, which knits together the strategic intent and larger objectives of the Network, the common agenda can be identified in the specific elements of the fusion center logic model. The NNFC's logic model captures with greater specificity the *how* of the NNFC's common agenda, the activity within and between centers, and the intended impact of the Network's operation in four general terms.

---

[111] "Fusion Center Performance Program (FCPP)," Department of Homeland Security, last updated August 14, 2014, http://www.dhs.gov/fusion-center-performance-program-fcpp.

[112] Department of Homeland Security, *National Strategy for the National Network of Fusion Centers*.

[113] Department of Homeland Security, *2013 National Network of Fusion Centers Final Report*.

- Inputs—resources provided to operate the NNFC
- Processes—the actual work completed by the NNFC
- Outputs—the product of the processes
- Outcomes—the benefit and/or impact of the efforts of the NNFC[114]

2. Shared Measurement

Considering the unique nature of a network comprised of vastly dissimilar components, and recognizing the need to create a standardized method of determining the maturity and robustness of the NNFC, two categories of network-wide capability, comprised of several common tasks provide a framework for measurement. Critical operational capabilities and enabling capabilities, not only assess capability, but also ensure the ability to perform tasks is aligned with the strategic intent of the NNFC.

The critical operational capabilities are the following.

- *Receive:* Ability to receive classified and unclassified information from federal partners.
- *Analyze*: Ability to assess local implications of that threat through the use of a formal risk assessment process.
- *Disseminate*: Ability to further disseminate that threat information to other state, local, tribal, territorial, and private sector entities within their jurisdiction.
- *Gather*: Ability to gather locally generated in formation, aggregate it, analyze it, and share it with federal partners as appropriate.

The enabling capabilities are as follows.

- *Privacy, Civil Rights and Civil Liberties (P/CRCL) Protections*: The ability and commitment to protect the P/CRCL of all individuals.

[114] Department of Homeland Security, *2013 National Network of Fusion Centers Final Report*.

- *Sustainment Strategy*: The ability to establish and execute a sustainment strategy to ensure the long-term growth and maturity of the network.

- *Communications and Outreach*: The ability to develop and execute a communications and outreach plan.

- *Security*: The ability to protect the security of the physical fusion center facility, information, systems, and personnel.[115]

3. Mutually Reinforcing Activities

It could be reasonably argued that each of the fusion centers in the NNFC, by virtue of their universally accepted mission, reinforces each other's activities and are united by a common set of goals as indicated in its national strategy. Further, through its development of homeland security standing information needs (HSEC SINS), the DHS has provided a framework of common information-gathering priorities for the NNFC. This framework, however, is not inflexible or arbitrary; understanding that each geographic area serviced by a fusion center faces unique issues, each center, based on its own assessment, formulates its own set of standing information needs (SINs) and priority intelligence needs (PINs) By sharing SINS and PINS between centers and the Network, regional or national collaborative partnerships can be formed among centers that have identified common priorities that can lead to joint intelligence production and enhanced efficiency.

4. Continuous Communication

Robust and ongoing communication throughout the NNFC is a necessity considering its information-sharing mission. It is executed through a variety of means, both in-person meetings, and technology solutions, such as the

[115] Department of Homeland Security, *Critical Operational Capabilities for State and Major Urban Area Fusion Centers: Gap Mitigation Strategy* (Washington, DC: Department of Homeland Security, December 2010), 3.

Homeland Security Information Network (HSIN),[116] to ensure that information flows both vertically and horizontally to all critical mission partners. In addition, organizations, such as the National Fusion Center Association and Southeast Regional Fusion Center Association, or "Southern Shield," advocate for national and regional priorities and participate in strategic planning for the network.

5. Backbone Support

Due to the wide and varied organization structure of fusion centers, each center may receive its backbone support from a different agency. However, on the larger scale, the national network receives its true backbone support from the Office of Intelligence and Analysis through the SLPO of the DHS. The SLPO provides individual centers in the network with the majority of guidance and assistance with capability and capacity building activities, including the following.

- Give technical assistance that can range from policy development to privacy reviews
- Provide security clearances and access to classified and sensitive but unclassified data systems
- Coordinate training deliveries for fusion center personnel and their critical mission partners
- Sponsor travel to attend collaborative meetings
- Assist with analytical capacity

[116] The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share SBU information. Federal, state, local, tribal, territorial, international, and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs. "Homeland Security Information Network (HSIN)," Department of Homeland Security, last updated July 17, 2014, http://www.dhs.gov/homeland-security-information-network.

F. CONCLUSION

As sharing national security information among the widest appropriate audience is a national priority, and is too large a job for any single organization to accomplish successfully, the NNFC is a prime example of how collective impact finds practical application. It could also be confidently stated that even though individual fusion centers tend to focus on issues specific to their area of responsibility, they understand that they are bonded to a larger strategic effort.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

Follow the evidence to where it leads, even if the conclusion is uncomfortable.

—Steven James

Considering the evidence presented in the forgoing chapters, it would be hard to deny that the principles of CI are practiced internally *within* RISS centers, HIDTA ISCs and the NNFC. This viewpoint stands to reason because these networks have well-defined missions, and have institutionalized their policies, processes, and procedures. Moreover, considering that each of these networks "touch" each other's missions, it would be constructive to examine how CI is being leveraged *between* these organizations and where opportunities exist for greater levels of collaboration.

A. COLLECTIVE IMPACT BETWEEN SELECTED ELEMENTS OF THE DOMESTIC INTELLIGENCE ENTERPRISE

1. Common Agenda

Perhaps the most obvious statement of common agenda appears on the DHS's website, which describes that the activities of RISS centers, HIDTAs, and fusion centers complement one another:

> As such, the missions of fusion centers, RISS centers, and HIDTAs are complementary and require on-going coordination. Knowledge, expertise, relationships, and information held by RISS centers is invaluable to assist fusion center partners in identifying and analyzing homeland security threats.[117]

and

> Both fusion centers and ISCs are responsible for protecting our nation by serving as valuable conduits for information sharing among federal, state, local and tribal agencies. Their missions are

[117] "Fusion Centers and RISS Centers," Department of Homeland Security, accessed June 26, 2014, http://www.dhs.gov/fusion-centers-and-riss-centers.

> not isolated; to the contrary, counterdrug and counterterrorism efforts both address specific criminal activities that impact our homeland security.[118]

2. Shared Measurement

Concerning areas in which RISS centers and HIDTA ISCs seem to measure their performance and impact quantitatively (e.g., number of arrests, seizures, etc.), fusion centers express their impact in a more anecdotal fashion, noting success stories, volume of analytical capacity, and added value. Since substantial commonality in mission occurs between these elements, the opportunity exists to develop a method of measurement, which focuses on the outcomes of activities that are identical across the enterprise.

3. Mutually Reinforcing Activities

Several examples of mutually reinforcing activities are available across the enterprise, the most consequential of which may be a recent project undertaken by a RISS center located in the northeastern United States, the NESPIN. NESPIN proposes the federation of the criminal intelligence databases from the 17 fusion centers in the region in an effort to share information seamlessly across the region using the RISSIntel platform.[119] Another similar, yet no less impactful action undertaken by the DHS and the RISS centers is the federation of their automated information-sharing platforms, the Homeland Security Information Network (HSIN) and RISSIntel. Finally, participation in groups, such as the Global Justice Information Sharing Initiative, the Criminal Intelligence Coordinating Council, and the Information Sharing Environment, even though compelled by law, still represents a major commitment to coordinate joint plans of action for common issues.

---

[118] "Fusion Centers and HIDTS Investigative Support Centers," Department of Homeland Security, accessed June 26, 2014, http://www.dhs.gov/fusion-centers-and-hidta-investigative-support-centers.

[119] *Northeast Fusion Center Intelligence Information Sharing Pilot Project*, June 28, 2013.

4. Continuous Communication

In line with the activities listed above, it would be expected that RISS centers, ISCs, and fusion centers remain in continuous communication and strive to build trust across the enterprise. One specific example of this ongoing effort is the fusion center network's unified message[120] relating to event, case, and investigative target disambiguation. Leveraging technologies provided both by RISS (RISSafe), and HIDTA (SAFETNet and Case Explorer), ISCs, fusion centers and RISS centers routinely share information to better focus investigative resources and enhance officer safety.

5. Backbone Support

Even though RISS centers, HIDTA ISCs and fusion centers' funding, chain of command, and program management mechanisms remain largely segregated, several associated organizations could be construed as "backbones." The IIR and the BJA both provide resources and skills to coordinate the efforts of the enterprise. Among many activities sponsored by IIR is invitational travel for fusion center leaders to attend HIDTA ISC workshops and the BJA's support of meetings and conferences provide opportunities for enhanced collaboration.

B. RECOMMENDATIONS AND TOPICS FOR FURTHER STUDY

This thesis has intended to frame three elements of the domestic intelligence enterprise that are primarily missioned to serve and provide information-sharing facilities for state and local partners in the context of CI. However, opportunities exist for further investigation and research, which are well beyond the scope of this work, may benefit each of the parties (RISS centers, HIDTA ISCs, and fusion centers) and increase the effectiveness and impact of their work. Additional areas of research will most likely involve a longer-term examination of specific activity, and will likely involve the collection and statistical

[120] In October 2013, 14 criminal intelligence-coordinating organizations, led by the national network of fusion centers, issued a call to action to enhance officer safety using event deconfliction systems.

analysis of large amounts of raw data, personal interviews, and meetings with several domestic intelligence stakeholders.

Some recommendations and possible areas for further research are listed as follows.

- Explore policy changes that would allow longer-range funding with respect to strategic, impactful goals rather than funding based on year–to-year volume.

  In the current model, funding is provided on a year-by-year basis, which limits strategic planning and long-term project development. In addition, some grant regulations prohibit contracts spanning longer than the grant's typical one-year cooperative agreement, which can limit strategic purchasing decisions especially in the information technology realm.

- Mutually shared collection and reporting priorities should be codified and areas of specialty should be established within and between members of the enterprise.

  Rather than building redundant capability, where practical, similar missions should be assigned to the organization best equipped and trained.

- The already strong relationships between practitioners should be leveraged to encourage funding agencies to streamline evaluation criteria and investment justification.

  A funding formula for elements with common or shared missions should be developed to encourage more joint funding and avoid funding redundant programs.

- Continue federation of information-sharing systems and duplicate the efforts currently being undertaken by NESPIN.

- Design a program of research and analysis along with a comprehensive battery of common metrics, which empirically represent the relationship between information sharing, collective effort and associated impacts on established goals and objectives.

Several metrics capture the volume of activity. However, these may only be a surrogate for real impact. A collection and analysis of the relationship between information shared and desired outcomes would be useful.

- Recognize that the value of competitive analysis between elements of the enterprise and develop a non-punitive "red team" process between elements. In addition, RISS centers and ISCs should be invited to participate in fusion center exercises.

C. CONCLUSION

No doubt exists that the domestic intelligence enterprise in the United States serves a very impactful purpose and the capabilities built have enhanced and encouraged collaboration on levels never before imagined. Whether established by legal mandate, in response to a crisis, or a natural need to cooperate, deliberate and planned collaboration has replaced most of the "random acts of partnership"[121] from the past. However, giving credit to the successes to date, any enterprise, which is so complex and has such a far-reaching mission, can benefit from the innovation and fresh inquiry collective impact offers.

[121] "The 'How To' Guide,' Collaboration for Impact," accessed July 15, 2014, http://www.collaborationforimpact.com/the-how-to-guide/.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Bardach, Eugene. *Getting Agencies to Work Together: The Practice and Theory of Managerial Craftsmanship*. Washington, DC: Brookings Institution, 1998.

Bush, George W. *The Department of Homeland Security*. Washington, DC: Department of Homeland Security, June 2002.

Carson, Emmett D. "Rethinking Collective Impact." August 31, 2012. http://www.huffingtonpost.com/emmett-d-carson/rethinking-collective-imp_b_1847839.html.

Collaboration for Impact. "The 'How To' Guide." Accessed July 15, 2014. http://www.collaborationforimpact.com/the-how-to-guide/.

Dahl, Erik J. "Domestic Intelligence Today More Security but Less Liberty?" *Homeland Security Affairs*, 7, The 9/11 Essays (September 2011): 1–9.

Department of Homeland Security. *2013 National Network of Fusion Centers Final Report*. Washington, DC: Department of Homeland Security, 2014.

———. *Critical Operational Capabilities for State and Major Urban Area Fusion Centers: Gap Mitigation Strategy*. Washington, DC: Department of Homeland Security, December 2010.

———. *Fusion Center and Emergency Management Collaboration Meeting After-Action Report*. Washington, DC: Department of Homeland Security, 2014.

———. "Fusion Center Performance Program (FCPP)." Last updated August 14, 2014. http://www.dhs.gov/fusion-center-performance-program-fcpp.

———. "Fusion Centers and HIDTA Investigative Support Centers." Accessed June 26, 2014. http://www.dhs.gov/fusion-centers-and-hidta-investigative-support-centers.

———. "Fusion Centers and RIIS Centers." Accessed June 26, 2014. http://www.dhs.gov/fusion-centers-and-riss-centers.

———. *NIMS Intelligence/Investigations Function Field Operations Guide*. Washington, DC: Department of Homeland Security, 2013.

———. *Performance Measures Definition Guide*. Ver. 1.0. Washington, DC: Department of Homeland Security, April 2014.

Department of Justice. *National Criminal Intelligence Sharing Plan*. Washington, DC: Department of Justice, 2003.

Executive Office of the President. *National Drug Control Strategy*. Washington, DC: HIDTA, Office of National Drug Control Policy, 2004.

Federal Bureau of Investigation. "Protecting America from Terrorist Attack, Our Joint Terrorism Task Forces." Accessed July 2, 2014. http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs.

Department of Justice. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: Department of Justice, 2006.

German, Mike, and Erik Dahl. "Intelligence Reform: Challenging the Conventional Wisdom Part 2." July 15, 2014. NPS Video.

Gibson, Chris. *Using SERVQUAL to Assess the Customer Satisfaction Level of the Oregon HIDTA ISC Analytical Unit*. Portland, OR: Hartfield School of Management, Portland State University, 2009.

Government Accountability Office. *Information Sharing. Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities* (GAO-13-471). Washington, DC: U.S. Government Accountability Office, 2013.

———. *Report to the Chairman, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate. Results-Oriented Government Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies* (GAO-06-15). Washington, DC: U.S. Government Accountability Office, October 2005.

Gutierrez, Michael J. "Intelligence and High Intensity Drug Trafficking Areas (HIDTA'S): A Critical Evaluation of the HIDTA Investigative Support Center." Master's thesis, Naval Postgraduate School, 2004.

Hanleybrown, Fay John Kania, and Mark Kramer. "Channeling Change: Making Collective Impact Work." *Stanford Social Innovation Review*, January 26, 2012. http://www.ssireview.org/blog/entry/channeling_change_making_collective_impact_work.

Hocevar, Susan Page, Gail Fann Thomas, and Erik Jansen. "Inter-Organizational Collaboration: Addressing the Challenge." *Homeland Security Affairs* 7, The 9/11 Essays (September 2011): 1–8.

Homeland Security Advisory Council. “Intelligence and Information Sharing Initiative, Homeland Security Intelligence & Information Fusion.” Department of Homeland Security, April 2005. http://www.dhs.gov/xlibrary/assets/HSAC_HSIntelInfoFusion_Apr05.pdf.

Institute for Intergovernmental Research. “Regional Information Sharing Systems (RISS).” Accessed July 15, 2014. https://www.iir.com/WhatWeDo/Information_Sharing/RISS/.

Joint Terrorism Task Force, The. “History of the JTTF.” Anti-Defamation League, 2005. http://archive.adl.org/learn/jttf/history_jttf.html.

Kania, John, and Mark Kramer. “Collective Impact.” *Stanford Social Innovation Review* 1, no. 9 (2011): 36–41.

Kean, Thomas H., and Lee Hamilton. *National Commission on Terrorist Attacks upon the United States, The 9/11 Commission report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004.

Long, Edward, and Aimee L. Franklin. “The Paradox of Implementing the Government Performance and Results Act: Top-Down Direction for Bottom-Up Implementation.” *Public Administration Review* 64, no. 3 (May–June 2004): 309–319.

Masse, Todd. *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States* (CRS Report No. RL31920). Washington, DC: Congressional Research Service, 2003.

Masse, Todd, Siobhan O’Neil, and John Rollins. *Fusion Centers: Issues and Options for Congress* (CRS Report No. RL34070). Washington, DC: Congressional Research Service, 2007.

Moore, Mark, and Sanjeev Khagra. *On Creating Public Value: What Business Might Learn from Government about Strategic Management, Corporate Social Responsibility Initiative Working Paper No. 3*. Cambridge, MA: John F. Kennedy School of Government, Harvard University, 2004.

Morag, Nadav. “Does Homeland Security Exist Outside the United States?” *Homeland Security Affairs*, 7, The 9/11 Essays (September 2011): 1–5.

Mucha, Michael J. “Organizational Alignment with Logic Models,” *Government Finance Review* 24, no. 5 (October 2008): 51–54.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. Washington, DC: U.S. Government Printing Office, 2004.

National HIDTA Directors Association, *HIDTA Program Summary 2012*. Alexandria, VA: National HIDTA Directors Association, 2012.

National Network of Libraries of Medicine. “Guide 5: Define How a Program Will Work—The Logi Model.” Last updated October 5, 2012. nnlm.gov/outreach/community/logicmodel.html.

National Strategy for the National Network of Fusion Centers. Department of Homeland Security, *National Strategy for the National Network of Fusion Centers*. Washington, DC: Department of Homeland Security, 2014.

Northeast Fusion Center Intelligence Information Sharing Pilot Project, June 28, 2013.

Office of National Drug Control Policy. *Design for a HIDTA/OCDETF Performance Monitoring and Management System*. Washington, DC: Executive Office of the White House, 2003.

———. *HIDTA Program Policy and Budget Guidance*. Washington, DC: Executive Office of the White House, 2012.

———. “High Intensity Drug Trafficking Areas (HIDTA) Program.” The White House, accessed May 1, 2014. http://www.whitehouse.gov/ondcp/high-intensity-drug-trafficking-areas-program.

———. “Intelligence and Information Sharing.” In *Program Policy and Budget Guidance*. Washington, DC: Executive Office of the White Office, 2009.

Randol, Mark A. *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress* (CRS Report No. R40602). Washington, DC: Congressional Research Service, 2010.

Regional Information Sharing Systems. *Regional Information Sharing Systems Annual Report*. Washington, DC: Regional Information Sharing Systems, 2013.

———.*Regional Information Sharing Systems Annual Report, ATIX Brochure*. Washington, DC: Regional Information Sharing Systems, 2013.

———. *Regional Information Sharing Systems Annual Report, Executive Summary*. Washington, DC: Regional Information Sharing Systems, 2013.

———. *Regional Information Sharing Systems Annual Report, RISSGang Brochure*. Washington, DC: Regional Information Sharing Systems, 2013.

———. “Frequently Asked Questions.” Accessed July 14, 2014. https://www.riss.net/Documents/RISS.FAQ.pdf.

———. “Frequently Asked Questions, How is RISS Funded?” Accessed July 15, 2014. http://www.riss.net/default/faq#7.

———. “Regional Information Sharing Systems (RISS) Program.” Accessed July 15, 2014. https://www.riss.net/default/Overview.

———. *Regional Information Sharing Systems Program History and Evolution*. Washington, DC: Regional Information Sharing Systems, 2013.

Relyea, Harold C., and Jeffrey W. Seifert. *Information Sharing for Homeland Security: A Brief Overview* (CRS Order Code RL32597). Washington, DC: Congressional Research Service, 2005.

Report to the Chairman, Subcommittee on Commerce, Justice, State, and the Judiciary Committee on Appropriations, United States Senate, Regional Information Sharing Systems (GAO/GGD-85-17). Washington, DC: General Accounting Office, 1984.

Schmid, Kurt. “A Foundation for Information Sharing.” *Police Chief Magazine* 70, no. 11 (November 2003).

Strive Partnership. “Quality Continuous Improvement.” July 15, 2014. http://www.strivepartnership.org/priority-area-highlights.

———. *Strive Partnership Report 2012–2013*. Cincinnati, OH: Strive Partnership, 2013.

Thompson, Chris. “Rereading Collective Impact: Three Lessons.” *Stanford Social Innovation Review*, February 3, 2014.

Treverton, Gregory F. “Reorganizing U.S. Domestic Intelligence, Assessing the Options.” RAND Corporation. Accessed November 16, 2013, http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG767.pdf.

U.S. Government Accounting Office. *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration Amount Federal Agencies* (GAO-06-15). Washington, DC: U.S. Government Accountability Office, 2005. http://www.gao.gov/new.items/d0615.pdf.

White House, The. *National Strategy for Information Sharing, Success and Challenges in Improving Terrorism-Related Information Sharing*. Washington, DC: The White House, 2007.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California